Big Brother and His Magic 8-Ball

A Legal Analysis of the Applications of Data Assisted Predictive Policing

By: Lawrence David Bushnell Jr.

MA In Policy Studies Capstone

University of Washington Bothell

August 13, 2020

Contents

Chapter 1: Introduction ……**02**

Chapter 2: Literature Review……**05**

Case Study: Chicago's Strategic Subjects List (SSL)……..**08**

Chapter 3: Methodology……**12**

Chapter 4: Legal Analysis……...**17**

Exclusionary Rule……**17**

Katz v. United States……...**24**

Third Party Exception……**28**

Emergent Technologies……..**35**

Applying the Framework……...**48**

Chapter 5: Conclusions and Recommendations……..**54**

Dedication:

This work is dedicated to my Father Lawrence David Bushnell Sr. and my Mother Lillian Lin Bushnell. Without their steadfast support over the last 25 years, none of this would be possible.

Abstract:

This paper investigates the relationship between predictive policing methods or so called "pre-crime," and Fourth Amendment protections. In the body of sociological research, the study of state observation and carceral power has been at the forefront of the field for the last several decades. Starting with Foucault and the resurgence of the panopticon, surveillance studies have sought to describe the relationship of the individual to power. The rapid advent of the internet over the last several decades has allowed for new and innovative surveillance methods to proliferate. Instead of the traditional closed-circuit-television (CCTV), internet service providers (ISPs), social media companies, and web browsers collect their user's data to create huge data sets curated by artificial intelligence. These so called "Big Data" sets are used by police to create predictive models for policing. These surveillance methods consist predominately of two modes, either predicting areas likely to play host to crime or predicting which individuals will likely commit crimes. For an emergent branch of sociological research, there is already a robust body of literature representing research conducted into the efficacy of such surveillance models; however, much of this research leaves out a critical component of criminal justice. That is the law. Instead of simply critiquing predictive policing, this paper sets out to demonstrate that the use of predictive policing methods is often a violation of protections around the Fourth Amendment. To do this, I use approximately the last 80 years of Fourth Amendment law to construct a framework to analyze the Constitutionality of the two primary forms of predictive policing methods. Many municipalities are beginning to move towards predictive methods, and this paper can serve as a cautionary guide to avoid the implementation of unconstitutional policing practices.

Chapter 1 Introduction:

The Minority Report by Phillip K. Dick was a novella published in 1956 which quickly captured the imagination of the American public. In this fictitious story, New York discovers members of its society which are able to see the future, particularly crimes, before they occur. The NYPD puts these "Precognatives" or precogs to work in a special division of the department aptly named Pre-Crime. The job of these precogs is to predict as accurately as possible the who, when, and where of future crimes, so officers can be dispatched to apprehend the suspect prior to the commission of the crime. While this story is a work of science fiction, reality is not far behind.

The last twenty years have seen an incredible rise in the use of the internet. According to Our World In Data, in 1990 approximately 2.6 million people used the internet, but by 2015 the world saw a 130,000% increase to a staggering 3.4 billion users (Roser, Ritchie, & Ortiz-Ospina, 2020). This exponential growth prompted the development of dozens of new technologies which have dramatically changed the quality of life for people in the first world. Online word processors have enabled people to keep documents secure and accessible at any point in the world, social media has allowed people to stay connected in ways that were impossible before the internet, and it has stoked the consumerist fuel of our economy through easy one-stop shopping with services like Amazon and Ali-Baba. However, all these various new technologies have a sinister side which is in the forefront of the western zeitgeist. Specifically, the balance of this new tech assisted lifestyle and privacy.

While these technologies have provided many benefits, they come with significant concerns related to personal privacy and data collection. Many internet service providers (ISPs) and

websites collect data on individuals. This data can include things such as browsing history, purchase history, social media posts, and much more. These private companies take the user's data and sells it to different marketing agencies to target advertisement towards consumers. This has become such common knowledge that according the Pew Research Center, 60% of Americans believe that it is not possible to go through daily life without having data collected by companies or the government (Auxier, Rainie, Anderson, Perrin, Kumar, & Turner, 2019). Additionally, according to the same study, most Americans report concerns over the use of their data.

Much of this concern is very well founded. In fact, many may remember the Cambridge Analytica scandal which broke in 2018. In this scandal, a whistleblower revealed how in 2014 "We exploited Facebook to harvest millions of people's profiles. And built models to exploit what we knew about them and target their inner demons. That was the basis that the entire company was built on"(Cadwalladr & Graham-Harrison, 2018). It is little wonder then, that many Americans are concerned not only with their privacy with just Facebook, but other companies engaging in this type of activity.

Cambridge Analytica is what is known as a "Data Broker." As Leetaru explained in their article in Forbes Magazine, "In the world of data brokers, you have no idea who all has bought, acquired or harvested information about you, what they do with it, who they provide it to, whether it is right or wrong or how much money is being made on your digital identity. Nor do you have the right to demand that they delete their profile on you" (Leetaru, 2018). Essentially, ISPs, browsers, and social media sites are not the end destination of your data. Data is collected by these institutions; however, it gets resold to data brokers who buy information from a

multiplicity of sources to create complete profiles on individuals, then resells these profiles to clients for a huge profit (Crane, 2018).

Among many other clients, data brokers sell their information to various government agencies, specifically to policing agencies (Crane, 2018).When people sign up for services such as ISPs, social media, and web browsers, the user typically must agree to a "Terms of Use" agreement, which of course everyone reads carefully. While it is true that we sign away the rights to our data, the terms of use frequently do not specify that this information will be passed on to government agencies. In this paper, I look at the use of big data sets collected by the government to implement predictive policing technologies. First, this paper will demonstrate many of the common critiques launched at predictive policing methods; however, most of these critiques do not address the means by which policing agencies collect this data. In the second half of this paper, a framework based on the last 80 years of Fourth Amendment Law will be tested against two predictive policing case studies from the Chicago Police Department.

Chapter 2: Literature Review:

New surveillance technologies have allowed for the blossoming of a multi-billion-dollar industry in which user data is purchased and sold. These "data brokers" operate with very little government oversight. Data Brokers buy datasets from ISPs, browsers, and social media to create complete profiles on individuals to resell to the highest bidder (Crane, 2018). Even if there was transparency with these organizations, it would fail to solve the problems that data-brokers present in the area of surveillance. Crain argued that data brokerage functionally commodifies humans and no amount of transparency will solve this. In this new economy, the workers are everyone, and we generate value for the data brokers. Crain uses a Marxist lens to evaluate this and demonstrates that the surplus labor (your data) is completely co-opted by data-brokers functionally rendering us slaves (Crane, 2018). Further, Smith Coined the term "Data Doxa" when discussing the gaze of data brokers. What Smith means by Data Doxa is the inescapable reality that the use of technology, and therefore by proxy the collection of data, are entrenched and intractable to the modern Western way of life (Smith, 2018). Building on both of these critiques, if data use is entrenched and thereby the use of data brokers is entrenched, it becomes of paramount importance to understand how this data is used.

This power relationship and analysis on gaze proposed by Smith is not a new concept in surveillance studies; however, it is important to understand how this theory is situated in the modern context of data surveillance. Mark Andrejevic writes extensively on modern surveillance and expands on much of the theoretical work that proceeded him. The goal of modern surveillance pivots away from Foucault's original notion of deterrence to pre-emption. He argued that with the growing ubiquity of surveillance, we begin to move away from the partial surveillance of the panopticon where inmates *could* be observed at any time, and move towards a

system of total surveillance where all the inmates are observed at all times. This in turn makes it possible for the observed to be constantly acted upon by an outside source. The operationalization of the automation of surveillance render the punishment aspect of surveillance moot. The ultimate goal of automatic surveillance is to pre-empt crimes before they happen. "In automated surveillance systems, the homogeneity of the disciplinary model is replaced by the continuous process of experimentation and environmental modulation calculated to generate more data and thus anticipate and foreclose through intervention" (Andrejevic, 2019). The purpose of my research is to investigate this operationalization of automated surveillance as it relates to these anticipatory methods.

Another seminal scholar who is necessary to reference when discussing data surveillance studies is McQuade. In his work Surveillance and Society, McQuade brings together Pfaffenberger's theory of "Technological Dramas" and Bourdieu's theory of "field." In this work, McQuade critiques the field of surveillance studies of failing after many years to move away from the theoretical discourse to the practical concerns therein. Essentially, while analysis of gaze and power is a fruitful discourse, and indeed a necessary one, this cannot be the end of it. It is necessary therefore to have discussion about the practical applications and means of resisting surveillance (McQuade, 2016). This paper attempts to use the framework set forth by McQuade to discuss and critique data surveillance in practice and not simply in theory. This work therefore attempts to ground itself in the theory of predecessors while attempting to bring real world application to the realm of data surveillance.

To investigate the uses of data, the first place to turn with any sort of surveillance is to look at how the state uses this information. Policing agencies around the world use data obtained from data brokers in their policing methods. In 2006 even before the advent of social media as we

know it today, the issue of data brokers was serious enough to warrant a federal investigation by the House of Representatives. In this investigation, it was shockingly revealed that many of the top federal law enforcement agencies, including the CIA, ATF, and FBI, all were accessing information from data brokers on a regular basis. Not only do federal agencies use data from data brokers, but local police precincts also obtain information from these firms (U.S. Congress, 2006). This information is used in data assisted predictive policing (DAPP) models across the country. Many cities have begun to implement DAPP models with varying levels of surveillance, intrusion, and success. In Florida, for example, the Florida judicial system uses DAPP to assist in the prediction of likely recidivism rates as a means of determining the length of a sentence for defendants found guilty of crimes (Asaro, 2019).

While much of the theoretical work done with data surveillance has been geared toward gaze analysis and other means of discursive rhetoric surrounding the issue, Chan & Moses identified 10 assumptions that predictive policing methodologies employ which need to be critiqued and investigated further. These assumptions are as follows: (1) Data use accurately reflects reality (2) The future is like the past (3) Irrelevance of omitted variables (4) Algorithms are neutral and do not inherit the biases of their coders (5) Data analytics does not unjustly discriminate (6) Primacy of place (geography over people) (7) Targeting police deployment should be the primary intervention (8) Perfect implementation (9) Changing police deployments prevents crime (10) The focus on crime is always appropriate. Additionally, Chan & Moses argued that there has not been any effective evaluation of either the process or outcomes of predictive policing. They use two case studies which demonstrate that the outcomes and processes of predictive policing do not have a statistically significant impact on stopping crimes. Finally, the authors looked at accountability. They argue that the use of predictive policing techniques enables law

enforcement officials to deflect questions of policing decisions onto the algorithm as opposed to taking ownership for decisions made (Moses & Chan, 2018). My paper seeks to address the processes of predictive policing by asking the question, is this even legal?

The Fourth Amendment of the U.S. Constitution states "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized" (U.S. Const., 1791). The question is then raised, does information obtained through third party data brokers constitute a violation of the Fourth Amendment? This paper seeks to address two specific Fourth Amendment questions. When the police obtain information through data brokers to be used in predictive policing, does this constitute a "search" as defined in the Fourth Amendment? Additionally, if evidence obtained through predictive policing leads to an arrest, is this information admissible at trial?

Case Study:

In order to answer the research questions posed above, it's necessary to establish a framework to understand how the courts approach Fourth Amendment Jurisprudence with regard to fact patterns and similar cases. While this issue has yet to be litigated at the Supreme Court, we can look to specific cases and uses of DAPP to draw our fact pattern for comparison. To this end, prior to establishing the legal framework, it is necessary to closely review the information in the case studies that the legal framework will be analyzing. For this purpose, this paper will be investigating the two different DAPP methods employed across the country in recent years.

The City of Chicago pioneered a model of DAPP by which they took some 48 factors including criminal history, convictions, known drug use or crimes, proximity to other crimes, locations, education, etc. The Chicago PD took this information and assigned each individual a score from 1-500 with 500 being most likely to commit a crime and 1 being least likely. The program was implemented in 2012, and involved approximately 400,000 individuals being actively tracked by the Chicago PD. Further, according to Peter Asaro, "While some 258 received the top score of 500 points, only 48% of these had previously been arrested for a gun crime, and many people on the list had never themselves been arrested, but rather were victims or were in the social networks of victims or perpetrators (Asaro, 2019). This "Strategic Subjects List" or SSL is the first model of DAPP we will be investigating through the use of the Fourth Amendment framework developed later in this paper.

The SSL was operationalized through several ways. During its initial roll-out, the Chicago PD failed to put in place any guiding policies which lead police officers to utilize the SSL in questionable ways. One of the most infamous methods of operationalization were the "Custom Notifications." Police officers would personally visit high risk subjects and inform them of their presence on the list and inform them that they would be at risk for increased police scrutiny. In his article *To Preempt a Thief* Andrejevic (2017) described one such visit:

> The movie *Minority Report* collided with the TV show *Person of Interest* for 22-year-old Chicagoan Robert McDaniel when a police officer showed up at his door one summer day to warn him not to get into trouble because the police were watching him. The warning was reportedly triggered by a predictive policing program used by the Chicago Police Department, a program that generated a "heat list."

Another way the SSL was operationalized was in the creation of the "Heat List" referenced in Andrejevic's article. The heat list was a list used after the perpetration of a violent crime that allowed the police to bring in "The usual suspects" in the vicinity of the crime for questioning. This led to people who were on the list being detained at rates far higher than the general public. According to Asaro, the presence on the list did not show a statistically significant correlation to the likelihood of individuals committing violent crimes (Asaro, 2019).

While the SSL model is used in Chicago, many other cities use a different form of DAPP. The second model of DAPP involves the use of historic crime data to create "heat maps" of areas more likely to suffer from crime which allows the police to dispatch to these areas and potentially prevent crimes from occurring. The first of these types of programs was implemented by the LAPD in 2008. LAPD rolled out two models of this program called LASER and PredPol. LASER was used to predict areas with a high likelihood of gun violence, while PredPol predicted likely property crime locations (Lau, 2020). Andrejevic, in the same article, presents an example of the effectiveness of this type of predictive policing stating "A Santa Cruz beat cop…was eating lunch in his patrol car in a downtown parking lot because it was on that shift's predictive list. He spotted two women trying to break into cars and arrested them" (Andrejevic, 2017). While this model of DAPP differs dramatically from the SSL model, it ought to come under the same scrutiny, especially if the data is obtained through data brokers.

A note on Transparency:

Policing agencies are notoriously uncooperative with the dissemination of information to the public. While it has been well documented that the police buy data from data brokers, the internal processes and operationalizations of this data is still largely a mystery. This ethic of

secrecy, or the “blue wall of silence” as it has been known to be called, is justified by law enforcement through the anti-circumvention argument. The Police argue that their methods must remain secret in order to keep criminals from circumventing their investigation techniques. Jonathan Manes critiqued this anti-circumvention argument in great detail in his work *Secrecy & Evasion in Police Surveillance Technology*. He argued that while the anti-circumvention argument is entrenched in police culture, it has not sustained any significant formal scholarly or court challenges. This anti-circumvention argument also undermines the systems of checks and balances that the country was founded on. “Secrecy impedes the ability of the courts to consider and adjudicate compliance with constitutional and statutory limitations because litigants will frequently be unable to mount court challenges to concealed techniques” (Manes, 2019). It is for this reason that it is unclear what policing agencies do with data obtained from Data Brokers. While it is possible that information used from data brokers are not used in DAPP, it can be inferred that the massive amounts of data necessary to conduct DAPP would necessitate the use of all available data, including that obtained from Data Brokers.

Chapter 3: Methodology

This study is a qualitative legal analysis of the development of the Fourth Amendment around emergent technologies, specifically DAPP. This analysis seeks to speculate based on historical data and context as to how the Supreme Court of the United States (SCOTUS) would handle a Fourth Amendment challenge to the use of DAPP. To test my hypothesis that the use of data brokers in DAPP is a Fourth Amendment violation, I will need to develop a framework based on prior fourth amendment litigation. Fourth Amendment law is a relatively new body of case law roughly one hundred years old. The data collected for this study will be the specific cases selected to create the framework based on the past eighty years of case law. The framework will focus primarily on what the SCOTUS has historically defined as protected under the Fourth Amendment. Once the framework is developed, I will test the two models of DAPP discussed above against this framework and determine if either of the models are legal under the current understanding of the Fourth Amendment.

Prior to the adoption of the framework, it is necessary to explain my methodology for selecting the cases to develop this framework. Given that the datapoints in this analysis are decided SCOTUS cases it is necessary to explain the logic behind the exclusion of some cases and the inclusion of others. While the question of DAPP has not been extensively litigated or questioned through rigorous legal analysis, there are several legal scholars and articles which do address these questions. These articles are where I began compiling a list of relevant opinions.

I began with a concept in Law that ties closely with criminal proceedings which is the "Exclusionary Rule". The Exclusionary Rule is derived from the Fourteenth Amendment which reads in relevant part "No state shall make or enforce any law which shall abridge the privileges

or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws" (U.S. Const., 1868). The application of this clause in legal proceedings results in the suppression of evidence, meaning that it cannot be submitted for consideration, when such evidence was obtained through a Constitutional violation. Andrew Ferguson, a legal scholar, wrote an article in the *Vanderbilt Law Review* relating "Blue Data" to the exclusionary. Ferguson argues in the article, that the gaze of surveillance from the police should be repurposed to foster data-driven police accountability in order to strengthen the exclusionary rule (Furguson, 2019). He used several cases in his analysis. In Herring v. United States and Utah v Strieff the courts established the modern understanding of the exclusionary rule as it exists today. Both these cases are related to the Fourth Amendment and the Exclusionary rule and were added to a list of potentially valuable cases.

Another article I discovered while researching the Fourth Amendment was written by Orin Kerr. While this article does not relate directly to the Exclusionary Rule, it does help identify other cases that could be helpful in the construction of the legal framework. In this article, Kerr proposed two ways regarding how the Fourth Amendment ought to be applied to the internet. First, he argues that the contents of online communications should be protected but that non-content information should not. Then he argues that courts should apply a warrant requirement to internet communications which target suspects as opposed to accounts (Kerr, 2010). While the first line of interrogation is interesting, it is less applicable to DAPP than the question of warrants. It is there that other cases which could be helpful in this legal analysis will be found. As Kerr points out in this article, the internet does not necessarily mirror the real world. Fourth Amendment law makes a distinction that Kerr describes as "Inside/Outside" distinction, which

will be covered in further detail in the framework proper. Suffice it to say that an individual has more Fourth Amendment protections on their private property than on public property. That is not to say that the Fourth Amendment does not apply to public property, but that individuals on private property have more protections afforded to them. To assist in the application of a new doctrine applicable to the internet, Kerr invoked three additional cases Katz v. United States, Olmstead v. United States, and Smith v. Maryland. These cases assist in the demonstration of the private/public distinction. This distinction is necessary to draw when assessing the Fourth Amendment, so these cases were added to the list of potential cases.

After reviewing these articles, I had a basic understanding of how the Fourth Amendment loosely interacts with data privacy. Additionally, all the articles referred to an important decision in Katz v. United States. It was clear that any Fourth Amendment analysis would be incomplete without a discussion of this case, so this was guaranteed a spot in the final framework. I then began to pull cases from Lexis Nexis, a premier research tool frequently used for researching case law. One of the many features of Lexis Nexis is the headnotes and footnotes often linked to individual opinions and cases. These frequently contain information critical to framing the case and understanding the jurisdictional history of the case prior to hearing at the SCOTUS. After a cursory search of cases related to "data," "privacy," and "social media" while filtering for SCOTUS cases I was able to identify several additional cases including Kyllo v. United states and Carpenter v. United States. Carpenter, while not specifically related to data brokers, was decided in 2018 which was the closest to a "case on point" (meaning the fact patterns are similar) that I found. Due to the applicability of this case, I combed through the cases referred to in the Majority opinion and added several additional cases to my list of potential briefs. These cases included the US. v. Miller, Smith v. Maryland, and United States v. Jones.

At this point, I had about twenty cases on my list of briefs from both the circuit court of appeals and the SCOTUS. I made a critical decision to cut the circuit court decisions from my cases. The reason for this is simple. Each circuit court covers a different jurisdiction for various parts of the United States. These create presidents only for the regions in question as such, a Ninth Circuit ruling will have no impact to law in the Sixth Circuit. Therefore, in order for the framework to be effective and applicable to the Federal Government and the country as a whole, it made the most sense to look at the Supreme Court whose rulings set precedence for the whole country as opposed to a specific region. This decision precluded about half of the cases that I had selected. The remaining SCOUTS cases were all necessary to create the framework so I chose to use all the remaining cases.

For each case I created a brief using the FAIR method of case analysis. FAIR stands for "Facts", "Action", "Issue", "Result/Rationale." The facts are the background of the case and the reason for the case in the first place. The action represents the jurisdictional history and the holdings of the lower courts, the issues are the questions being investigated by the court, and the result is the result and rationale of the case. After spending several days briefing these cases, I ordered them chronologically in a single document to better understand the logical flow of information. This was remarkably helpful in understanding how each opinion built upon the logic of the prior opinion all culminating in the Carpenter v. United States decision. It also revealed that the cases used in this framework can be divided into four distinct categories. The first is the development of the Exclusionary Rule specifically related to the Fourth Amendment and consists of three cases: Wolf V Colorado (1949), Irvine v. California (1954), Mapp v. Ohio

(1961). The second category is the case of Katz v. United States (1967). This case marked a dramatic departure from the conventional wisdom surrounding the application of the Fourth Amendment and deserves in depth analysis as to the implications of the decision in Katz. The third category deals with litigation of the Fourth Amendment related to information in the possession of third parties. These cases detail specific exceptions to the Fourth Amendment when the information is controlled by third parties and consists of two important cases US v. Miller (1976) and Smith v. Maryland (1979). The final category relates the Fourth Amendment to emergent technologies in the late '90s and 2000s. These cases enumerate exemptions to the Third Party Doctrine and establish how the SCOTUS treats emergent technologies. This is crucial for our analysis of DAPP as this utilizes emergent technologies. These cases consist of Kyllo V. United States (2001), United States v. Jones (2012) and Caprenter v. United States (2018).

Once all nine cases and their implications are discussed, a legal framework will be constructed by which it is possible to test the two DAPP initiatives listed above. It will combine the logics used in the federal opinions to determine what fact patterns are likely to get a case overturned at the federal level. When testing the DAPP initiatives against the framework, it should be possible to compare the facts of the case and determine whether the case would be thrown out for a Fourth Amendment Violation on a more-probable-than-not basis.

Chapter 4: Legal Analysis

In order to test the constitutionality of DAPP it becomes necessary to establish a framework by which it is made possible to determine whether an exertion of a claim to protection by The Constitution is in fact supported by law. In order to construct this framework, it is necessary to look at several seminal cases in the last 80 years of Fourth Amendment Law. Fourth Amendment law can be separated into two distinct eras separated by the 1967 decision of Katz which segregated property rights and the Fourth Amendment. This case marks a significant shift in the opinion of the Supreme Court of the United States (SCOTUS) and has been cited in nearly every Fourth Amendment case that followed. Additionally, in order to construct this framework, it is necessary to investigate the application of the Fourteenth Amendment's exclusionary rule (Right to a Fair trial) and whether the admission of evidence found in violation of the Fourth Amendment automatically constitutes a violation of the Fourteenth Amendment. There are a group of cases that have enumerated certain exceptions to the Fourth Amendment. These cases assess when third parties have access to documents whether the documents in question are considered protected under the Fourth Amendment. Finally, the SCOTUS in the last ten years have begun to regulate the use of emergent surveillance technologies such as GPS trackers and Cell Site Location Information. Each of these sets of cases comes together in order to form a cohesive framework by which it is possible to analyze whether the use of data brokers in DAPP constitutes a violation of the Fourth Amendment.

The Exclusionary Rule

The first set of cases to investigate are those surrounding the interplay between the Fourth and Fourteenth Amendments. Most of these cases were argued before the adoption of the Katz

opinion which means that at the time, Fourth Amendment law was closely tied to trespass. The Fourth Amendment only protected people from intrusion into their physical property and there was no assumption of a citizen's reasonable expectation of privacy. As such, the question prior to Katz was one of how and when to enforce the Fourth Amendment. One major concern during this time period was that this loophole would allow guilty criminals to get off while unjustly punishing law enforcement officers for doing their jobs. Another guiding doctrine was that the Fourth Amendment only applied to federal authorities and not state and local police.

The majority of the cases surrounding the Exclusionary Rule used for this framework were decided by the Warren Court (1953-1969) under Chief Justice Earl Warren. The Warren Court is often argued to be one of the most influential periods of SCOTUS history and is well remembered for its advocacy of civil rights. Under the Warren Court municipal facilities on public land were banned (1954), segregated public transportation laws were banned (1956), and segregated parks, playgrounds, and beaches were outlawed. In 1958 in Cooper v Aaron all nine justices recommitted to their decision in Brown v. Board of Education (Neuborne, 2010). It was during this era of expansive civil rights reform that the supreme court tied the Exclusionary Rule of the Thirteenth amendment to the doctrine of the Fourth Amendment. This is unsurprising as the Warren Court was committed to expanding the protections of the Constitution.

The first case to look at is Wolf v. Colorado (1949). This pre-Katz case upholds the doctrine set forth in an earlier case Weeks v. United States which stated that Fourth Amendment protections only applied to federal authorities, and left the decision to the states to determine how they would properly prosecute Fourth Amendment violations in their police forces. In doing so, it affirmed that a Fourth Amendment violation does not automatically constitute a violation of

the Fourteenth Amendment. In later opinions, the Weeks and Wolf decisions have been largely discredited.

In Wolf, the defendant was convicted of a state offense in a state court that had admitted evidence which was obtained through a violation of the Fourth Amendment. The specific question the court sought to answer was, in the words of justice Frankfurter, "Does a conviction by a State court for a State offense deny the 'due process of law' required by the Fourteenth Amendment, solely because evidence that was admitted at trial was obtained under the circumstances which would have rendered it inadmissible in a prosecution for violation of a federal law in a court of the United States because there deemed to be an infraction of the Fourth Amendment?" (Wolf v. Col., 1949).

Justice Frankfurter's opinion would go on to make three key arguments as to why a violation of the Fourth Amendment does not imply a violation of the Fourteenth Amendment. First, Justice Frankfurter argued that "The notion that the 'due process of law' guaranteed by the Fourteenth Amendment is shorthand for the first eight amendments of the Constitution and thereby incorporates them has been rejected by this court again and again" (Ibid). What Justice Frankfurter means by this is that while you may have the protections afforded by the first eight amendments, a violation of these protections does not intrinsically constitute a violation of the Fourteenth. This leaves the defendant with no real remedy to a violation of their constitutional rights.

The second argument that Justice Frankfurter put forth is the Common Law argument. Under Common Law, a system of law imported from England, holds that an unreasonable search and seizure constitutes a trespass of some kind. The police must produce a warrant when conducting

a search without probable cause, otherwise it is a trespass. Additionally, he argues that even when the police do commit a trespass in the course of their duties, it is not the place of the SCOTUS to set a punishment. He writes "How such arbitrary conduct should be checked, what remedies against it should be afforded, the means by which the right should be made effective, are all questions that are not to be so dogmatically answered as to preclude the varying solutions which spring from an allowable range of judgement on issues not susceptible of qualitative solutions" (Ibid).

Finally, Judge Frankfurter argued that the admission into evidence of information gained through an illegal search is not vital to the protection of privacy. He states that while the search may be illegal, this should not keep the evidence from being submitted for trial. Doing so would violate the Fourteenth amendment as evidence that could bring a criminal to justice would be excluded. While the decision in Wolf v. Colorado seems rather foreign under the current common understanding of our jurisprudence, Judge Frankfurter's rationale for his opinion is highlighted in another case. The case of Irvine v. California demonstrates that there is some value in this archaic interpretation of the Fourteenth Amendment.

In Irvine v. California, the Petitioner was convicted in a California state court for bookmaking and gambling on horse races in violation of the California anti-gambling laws. The police, suspecting the Petitioner of these illicit activities, made a copy of the key to the petitioner's house, and entered on multiple occasions to install, conceal, and reposition a microphone without a warrant. At trial, the Petitioner objected to the submission of the recordings, but the trial judge allowed the testimony of police officers to testify to the veracity of the statements made in the recordings (Irvine v. California, 1954). Additionally, the Petitioner was arrested with a federal

wagering tax stamp; certification of taxes paid for gains from gambling. The Petitioner was convicted, and the 9th Circuit Court of Appeals upheld the conviction.

On Certiorari to the SCOTUS, Judge Jackson delivered the majority opinion of the court. In his opinion, Judge Jackson stated, "Few police measures have come to our attention that more flagrantly, deliberately, and persistently violated the fundamental principle declared by the Fourth Amendment as a restriction on the federal government" (Ibid). Even still, Judge Jackson refers to the opinion of Wolf v. Colorado to indicate that the gross violation of the Fourth Amendment does not warrant overturning the case. The court decided to uphold the conviction for two reasons both contained in the opinion of Wolf v. Colorado. First, the officers who transgressed the Fourth Amendment rights of the petitioner were in fact state officers and not federal agents. As such, the opinion of Wolf gives the impetus on the states to develop means of punishing officers which transgress the Fourth Amendment, and does not allow any remedy from the courts, much less the SCOTUS. Further, Judge Jackson argued that:

> It must be remembered that petitioner is not invoking the Constitution to prevent or punish a violation of his federal right recognized in Wolf or to recover reparations for the violation. He is invoking it only to set aside his own conviction of crime. That the rule of exclusion and reversal results in the escape of guilty persons is more capable of demonstration that that it deters invasion of right by the police […] Rejection of the evidence does nothing to punish the wrong-doing official, while it may, and likely will, release the wrong doing defendant. (Ibid)

Essentially, Judge Jackson affirms the decision in the prior decisions of Wolf and Weeks as he felt there was no action the SCOTUS could take in order to sanction the state officials responsible for violating the petitioner's Fourth Amendment rights. Since the Petitioner was arrested with incriminating evidence on their person, the court was concerned that setting aside the conviction would only set free a guilty person while doing nothing pragmatically to rectify the Fourth Amendment violation.

This decision also upholds the decision found in Wolf in which it was determined that the Fourteenth Amendment is not simultaneously violated when evidence is presented that was obtained through a violation of the Fourth Amendment. Therefore, while the evidence was obtained illegally, the petitioner's Fourteenth Amendment protections to a fair trial were not violated. Again, while this understanding of the Fourth and Fourteenth Amendments may seem foreign to our modern understanding, these opinions help demonstrate the history of the Fourth Amendment, and how it has grown to protect more than a simple right to private property. Both the Wolf and Irvine opinions expressed that it was up to the states to sanction officers for violating the Fourth Amendment. It wasn't until the 1961 case Mapp v. Ohio that the Exclusionary Rule was finally tied to the Fourteenth Amendment.

In Mapp v. Ohio, the Petitioner Mapp lived on the top floor of their two-family home. Upon receiving information that a person of interest, wanted for questioning, was hiding out at Mapp's house, three Cleveland police went to investigate. Upon announcing their arrival, the Petitioner called her attorney who recommended refusing to admit the Police without a search warrant. After waiting for three hours, the police again sought entry to the Petitioner's residence. When she failed to immediately respond, the police breached the door and forced entrance. Shortly after the breach, the Petitioner's Attorney arrived, but the officers at the scene refused to allow

him to see his client, the Petitioner. While the police found no evidence of the person alleged to be hiding out in the house; they did uncover "certain lewd and lascivious books, pictures, and photographs in violation of Ohio's revised code" (Mapp v. Ohio, 1961). The petitioner was convicted in state court and the state supreme court affirmed the conviction on the basis that the Fourteenth Amendment did not apply in the state court's prosecution of the defendant for a state crime in accordance with Wolf.

In the opinion delivered by justice Clark, he articulated the reasons as to why the guiding doctrine of Wolf should be dismantled.

> Today we once again examine Wolf's constitutional documentation for the right to privacy free from unreasonable state intrusion, and, after its dozen years on our books, are led by it to close the only courtroom door remaining open to evidence secured by official lawlessness in flagrant abuse of that basic right, reversed to all persons as a specific guarantee against that very same unlawful conduct. We hold that all evidence obtained by searches and seizures in violation of the Constitution is, by that same authority, inadmissible in a state court (Ibid).

This obviously was a dramatic departure from the principles guiding the application of the Fourth Amendment up to this point. This opinion did two things for Fourth Amendment law. First it made it so that evidence seized in an illegal search or seizure was inadmissible in court; however, it leaves the rules of evidence obtained in a legal search still admissible. In Irvine, this means that the Federal Wagering Tax Stamp would have been admissible into evidence while the

recordings were not. This helps assuage the concerns of the court that a guilty criminal would be released from custody over an error in process. Additionally, it was established that the Fourth and Fourteenth amendments are not mutually exclusive. In general, if evidence is obtained thorough an illegal search and allowed to be admitted to evidence during criminal procedures, it is incumbent on the higher courts to overturn any subsequent conviction. The admission of evidence obtained through an illegal search is automatically a violation of the Fourteenth Amendment's guarantee to a fair trial.

Katz v. United States

Up until this point, the Fourth Amendment was linked to individual's property rights and not based on a reasonable expectation of privacy. In 1967, however, this all changed with the opinion of Katz v. United States. Katz fundamentally changed how Fourth Amendment Jurisprudence is analyzed by the Courts and marked a turning point in American Jurisprudence. Under the traditional understanding of the Fourth Amendment, citizens were protected from unreasonable search or seizure in an attempt to keep a person secure in their 'property, papers, and effects' meaning their private property. After the adoption of Katz, the Fourth Amendment would guarantee a 'reasonable expectation of privacy.' Additionally, Judge Harlan's concurrence in this opinion would set up a two-pronged test to establish such expectation of privacy, and this test is still in use today when analyzing Fourth Amendment questions. This decision comes at the tail end of the Warren Court (1953-1969) and predictably follows the Warren Court's prior decisions to expand the protections afforded by the Constitution.

In Katz, the Petitioner was found guilty of violating a federal statute prohibiting the transmission of wagering information by telephone. The FBI agents who were investigating the

case placed a listening device on the outside of a phone booth that the Petitioner was known to use without first obtaining a warrant. At trial, the petitioner filed a motion to suppress the evidence obtained through the listening device, but the trial court determined that since it was a public telephone booth, the petitioner was not protected by the Fourth Amendment. The court of appeals affirmed the decision of the trial court based on the fact that there had been no entrance into an area occupied by the defendant. The SCOTUS reversed the lower courts' decision finding that a person in a telephone booth could rely upon the protection of the Fourth Amendment. (Katz v. United States, 1967). While the SCOTUS was investigating the question of whether a public telephone booth is a constitutionally protected area, the larger question was whether physical penetration of a constitutionally protected area is necessary before a search and seizure can be said to have occurred.

In the opinion written by Justice Stewart, he opined on both questions before the court. In response to the first question, the constitutional status of the use of a phone booth, he declines to opine on the specifics as the court found that this was not the proper formulation of the question at hand.

> The petitioner has strenuously argued that the [phone] booth was a 'constitutionally protected area.' The government has maintained with equal vigor that it was not. But this effort to decide whether or not a given 'area,' viewed in the abstract, is 'constitutionally protected' deflects attention from the problem presented by this case. For the Fourth Amendment protects people, not places […] But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected (Ibid).

What Justice Stewart is arguing here is that the question of whether or not the phone booth is a constitutionally protected area is too narrowly tailored a question for this case. The heart of the case doesn't lie in whether the phone booth itself is constitutionally protected, but where the intent of the Fourth Amendment truly lies. To that end, Justice Stewart rejected the formulation of the question of both the Petitioner and the Government stating that "The Fourth Amendment protects people not place." Justice Stewart recognized here that the historical interpretation of the Fourth Amendment, though intended to protect citizens, really resulted in the protection of citizens' property and not the citizens themselves. Given Judge Stewart's rejection of the formulation of this case, he moved on to answer the second question, whether or not a Fourth Amendment violation requires some trespass into an area without a warrant.

Justice Stewart goes on to point out that the crux of the Government's case lies in the assumption that no "physical penetration" of the telephone booth occurred and that the listening device was placed on the outside of the booth. Further, the Government argued that since the telephone booth was made of glass and the occupant visible to the public, there was no difference between placing the call in the booth or on the street. The Justice was not impressed with these arguments. In response to the first question, Justice Stewart pointed to two earlier cases which had begun to decouple property rights from the Fourth Amendment. First, he pointed to Olmstead v. United States which the Government used to argue that surveillance without any trespass and without the seizure of any material object fell outside the protections of the constitution and rejects the Government's understanding of that case. Judge Stewart then proceeds to point to Warden v. Hayden in which the SCOTUS had begun dismantling the idea that property interests control the right of the government to search an area. On these two points, the SCOTUS rejected the government's case.

Finally, the Katz opinion established a specific right to privacy against government intrusion. Justice Stewart acknowledged that while the Fourth Amendment protects specific rights to privacy, it cannot be said to establish a general right to privacy as the Amendment extends protections beyond privacy and to limit the Amendment to a general right to privacy would ultimately restrict the protections afforded by the amendment. While Justice Stewart did not expand on this in his opinion, in Justice Harlan's concurrence, he establishes a two-pronged test to determine if an individual has a "reasonable expectation of privacy."

> There is a twofold requirement [to establish a reasonable expectation of privacy], first that a person have exhibit an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." Thus a man's home is , for most purposes, a place where he expects privacy, but objects, activities or statements that he exposes to the "plain view" of outsiders are not "protected" because no intention to keep them to himself has been exhibited.[…] The critical fact in this case is that "one who occupies it [a telephone booth] shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume" that his conversation is not being intercepted (Ibid).

This two-pronged test would go on to become the standard to determine whether a reasonable expectation of privacy exists, and if so whether the government intruded upon it when conducting a search. In this case, the Petitioner fulfilled the first requirement of a subjective expectation of privacy by using the booth and closing the door behind him. The second requirement was fulfilled by the fact that society in general would likely be willing to agree with the Petitioner that there was an expectation of privacy in the manner they used the phone booth.

Finally, while it was ruled that the Government's search was a violation of the Fourth Amendment, the court was careful to establish that pursuant to a warrant, the search would have been valid.

While the results of Katz would fundamentally change Fourth Amendment jurisprudence for decades to come, the "reasonable expectation of privacy" doctrine would undergo further scrutiny. For the purposes of this framework, it is important to look at one such exception which is the third-party exceptions.

The purpose of this framework is to determine whether the use of data brokers in DAPP is a violation of the Fourth Amendment. After Katz, the SCOTUS needed to establish whether individuals have a constitutionally protected expectation of privacy when their information is controlled by third parties. For the most part, there is no reasonable expectation of privacy when information is controlled by a third party. There are two cases that establish the doctrine of the third-party exception to the Fourth Amendment.

Third Party Exception

The two cases this framework employs to establish the Third Party exception fell under the jurisdiction of the Burger Court (1969-1986). Both these cases marginally walk back the expansion of the Fourth Amendment established in Katz. Among other notable cases, the Burger court presided over the case of the United States v. Nixon after the Watergate scandal establishing that no person, not even the president, is above the law. Additionally, the Burger court presided over the case of Roe v. Wade a case that still impacts political discourse to this day. At face value it may seem that the Burger Court continued the social justice legacy of the Warren Court, but this is not quite accurate. The difference is most starkly noted in the rationale

behind the Roe v. Wade decision. In the late 60's through the early 70's the question of legalizing abortion came to the forefront of the American consciousness for the first time. While several cases led up to the Roe decision, the Justices finally came to the consensus that it was necessary to expand the right of privacy to protect the mother and her doctor as opposed to creating a new right to abortion (Garrow, 2014). This departs from the Warren Court's doctrine of expanding rights by tempering it with a strict constitutional lens. In contrast, the Warren court would have likely explicitly expanded the rights of the mother. In Katz the Warren Court created a new right, a reasonable expectation of privacy. In Roe, the Burger Court took a different approach. While their reasoning still expanded rights, the Burger court was in many ways more tempered than the Warren Court and explicitly linked their reasoning to the Constitution as opposed to extending the logics of prior cases (Ibid). This explains why they placed restrictions on Katz v. United States with respect to third party information.

The first of these cases is the U.S. v. Miller which initially created this third party doctrine. In this case, the Bureau of Alcohol, Tobacco, and Firearms (ATF) issued grand jury subpoenas to the presidents of the banks where the defendant (Miller) kept his accounts. These documents assisted in obtaining the conviction of the defendant for operating an alcohol distillery without paying the appropriate federal taxes. On appeal, the circuit court found that the defendant had a reasonable expectation of privacy and that the documents should have been suppressed. The government appealed the decision, and the SCOTUS granted certiorari. The question the court was asked to resolve was whether bank records are protected under the Fourth Amendment (U.S. v. Miller (1967).

In typical SCOTUS fashion, Justice Powell did not directly answer the question, but established a guiding principle to help lower courts deal with similar fact patterns. In this case,

the defendant, Miller, asserted that the subpoenas issued were signed by a United States Attorney rather than a court. The court of appeals reversed the conviction on the basis that forcing the defendant to produce incriminating documents through a subpoena was a violation of both the defendant's Fourth Amendment protections to unreasonable search and seizure and Fifth Amendment protections against self-incrimination. The crux of this argument lies in the fact that the ATF issued the subpoenas to the bank presidents and not the defendant. Justice Powell quickly dismantled this argument by pointing to the Bank Secrecy Act which holds that bank records are controlled by "existing legal process." As Justice Powell put it "On their face, the documents subpoenaed here are not respondent's 'private papers unlike the claim in Boyd, respondent can assert neither ownership nor possession. Instead, these are the business records of the banks" (US v. Miller, 1976). Since the documents subpoenaed were under control of the bank, this did not constitute a Fourth and Fifth Amendment violation as the subpoenas were determined to constitute adequate legal process.

The defendant, Miller, also argued that he had a Fourth Amendment interest in the bank documents as they were copies of his personal records which were made available to the banks for a limited purpose. In this argument, the defendant relied on the opinion of Katz v. United States to establish an expectation of privacy. Justice Powell dismantled this argument as well formally applying third party exemption to Katz. Powell pointed out that in the Katz opinion the SCOTUS stressed that "What a person knowingly exposes to the public is not a subject of Fourth Amendment Protections" (Katz v. United States, 1967). Essentially, if a person gives information to a third party, the first prong of the Katz two pronged test is not met. The person expressing Fourth Amendment interests does not have a subjective expectation of privacy and therefore

does not have a reasonable expectation of privacy as the information has been given to a third party. Judge Powell expressed this concept as follows:

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed (US v. Miller 1976).

In this case, the SCOTUS ruled on four key points. First, it held that the subpoenaed materials were business records of the banks and not the respondent's private papers, thus keeping them from protection under the Fourth Amendment. The Court also held that there is no legitimate expectation of privacy in the contents of the original checks and deposit slips, since the checks are not confidential communications, but are transactions that occur as part of a bank's regular business. Additionally, the court held that the issuance of a subpoena does not violate a defendant's rights, even if a criminal prosecution is being considered at the time of the subpoena's issuance. Finally, the Bank Records Act's statute was controlled by "[The] existing legal process" meaning that a subpoena which was obtained through the normal channels is sufficient to compel a bank to turn over the requested information. Ultimately, this case established that an individual who knowingly and willingly gives their information to a third party relinquishes any subjective expectation of privacy as necessitated by the two-pronged test in Katz.

Another case closely related to the third-party doctrine and Katz is the case of Smith v. Maryland. This was the case which officially recognized the two-pronged test which was established in Judge Harlan's Katz concurrence as the test by which Fourth Amendment assertions to a "reasonable expectation of privacy" is tested. Additionally, this case strengthened the third-party doctrine related to Fourth Amendment claims and the use of telephones. In essence, similar to Miller, information that is controlled by a third party does not constitute protected information under the Fourth Amendment; in addition, it expands on this indicating that information that is designed to be shared, regardless of the location of that information, is not protected under the Fourth Amendment.

In this case, a woman in Baltimore was robbed by a man who fled in a 1975 Mote Carlo. After the robbery, the victim received numerous phone calls from an unknown man who identified himself as the robber. During one such call, the alleged robber asked her to step out of her house which she complied with. As she stepped out of her house, she saw the 1975 Mote Carlo slowly rolling past. Days after, while patrolling the victim's neighborhood, the police identified a 1975 Monte Carlo that met the victim's description. The officers traced the license plate back to the petitioner, Smith. After identifying the likely culprit, the police installed a pen register, a device used to track the numbers dialed from a telephone, at the central office of the telephone company. The police failed to obtain a warrant or court order prior to the installation of said pen register. The pen register revealed a call to the victim on the day it was installed, and the Petitioner was taken into custody and convicted (Smith v. Maryland, 1979).

During the trial, the Petitioner attempted to suppress "all fruits derived from the pen register" since the police had failed to obtain a search warrant. The trial court denied the motion to suppress stating that the installation of a pen register was not a violation of the Fourth

Amendment. The Maryland Court of Appeals held that there is "no constitutionally protected reasonable expectation of privacy in the numbers dialed into a telephone system," (Ibid) and affirmed the trial court's decision. The SCOTUS granted certiorari to answer the question are the numbers dialed into a phone protected under the Fourth Amendment?

The SCOTUS determined that the numbers dialed into a telephone are not protected under the Fourth Amendment. Justice Blackmun delivered the opinion of the court making three key points. First, Justice Blackmun officially recognizes the two-pronged test set forth in Katz. He point's to Justice Harlan's concurrence and cites that in order for a petitioner to exert their fourth amendment rights, they must exhibit a reasonable expectation of privacy. This is categorized by the Petitioner first having a subjective expectation of privacy and also that this expectation must be one that society is prepared to recognize as reasonable (Katz v. United States, 1967). The SCOTUS ruled that the Fourth Amendment did not cover telephone numbers dialed into a phone as the petitioner failed to demonstrate a right to privacy that society was prepared to recognize as reasonable. Justice Blackmun proceeded to tease apart the specific fact pattern of the case. He pointed out that the pen register was installed on telephone company property, so the Petitioner could not assert any penetration into his property. Further, Justice Blackmun points out that "Pen registers do not acquire the contents of communications. Given a pen register's limited capabilities, therefore, petitioner's argument that its installation and use constituted a "search" necessarily rests upon a claim that he had a 'legitimate expectation of privacy' regarding the numbers he dialed on his phone" (Smith v. Maryland, 1979).

In order to rise to protection under the Fourth Amendment, the petitioner was required to demonstrate that they fulfilled the requirements set forth in Katz. The petitioner argued that since he exclusively used the telephone in his house to dial the numbers, he had a subjective

expectation of privacy; however, the court held that this was asserted in error. Justice Blackmun wrote that the site of the call is immaterial to any question of Fourth Amendment protections. "Regardless of his location, petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete the call. The fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference, nor could any subscriber rationally think it would" (Ibid). Additionally, Justice Blackmun argued that since the numbers dialed into the phone are handed over to third parties, this was not a right to privacy that society was ready to recognize. This point was emphasized by the Justice who pointed out a multiplicity of ways by which it is expected that phone companies regularly collect information on the numbers being dialed while not listening to the contents of conversations. The numbers, he argues, are a necessary part off telephonic communication, and are regularly given out to third parties and members of the public. As such, there can be no legitimate claim to an expectation of privacy that is recognized under the Fourth Amendment.

Smith v. Maryland did two key things for Fourth Amendment Jurisprudence. It formally recognized the two-pronged test employed by Judge Harlan's concurrence in Katz, but it also further strengthened the third party doctrine by indicating that when a third party is involved neither of the two prongs of the Kats Test is fulfilled. As such, information made available to third parties is not protected under Fourth Amendment law; however, as law is convoluted, an exception to this rule exists in the final body of law investigated for this framework. This final body of Fourth Amendment law has to do with emergent technologies. In the 80 year time-frame of cases that were investigated for the purposes of this legal framework, technology had remained fairly stagnate, but the 90's and 2000's ushered in an era of rapid technological

expansion with the proliferation of the personal computer, cell phones, and other technologies. These emergent technologies posed many difficulties to the SCOTUS.

Historically, the SCOTUS tends to move incrementally and avoid large sweeping reforms which could be misconstrued as extrajudicial law making. However, with the abilities of computers and other emergent technologies rapidly outstripping the protections afforded by the Constitution, the SCOTUS has been forced to litigate many cases around emergent technologies. These cases are critical for the examination of data broker's relationships with policing as all the stakeholders in this policing system use highly advanced technologies. Understanding how the court is dealing with these technologies will inform how this legal framework applies to the legality of predictive policing methods.

Emergent Technologies

These three Emergent Technology cases were decided by two different courts. The first, Kyllo v. United States (2001) was decided under the Rehnquist Court whereas United States v. Jones (2012) and Carpenter v. United States (2018) were both decided by the current Roberts Court. The Rehnquist Court marks a turning point toward a much more reactionary conservative court. While there are certainly opinions that are more liberal leaning ie. Planned Parenthood v. Casey (upholding Roe v Wade with some modifications), overall the Rehnquist is certainly the most conservative in the years covered by this framework. Of the nine justices, only two took the liberal side with any regularity. The conservative nature is highlighted in the fact that the Rehnquist court regularly resists attempts to establish and expand new constitutional rights. (Bryden, 1992). In light of this context, it makes sense that in the case of Kyllo v. United States the Rehnquist court would add another criterion on top of the two-pronged test established under

Katz. This falls in line with the Rehnquist position of narrowing the scope of constitutional protections expanded by the Warren and Burger Courts.

The first case to begin the investigation of this third era of Fourth Amendment Jurisprudence is that of Kyllo v. United States. This case took the two-pronged test from Katz and added a new criterion for emergent technologies. If a person is able to fulfill the two pronged Katz test, and the surveillance technology used is not available to the general public, then any search conducted with the piece of technology and not supported by a warrant is considered an illegal search under the Fourth Amendment.

In this case, the Petitioner, Kyllo, was suspected of growing Marijuana. Police officers, familiar with the process of growing marijuana indoors, knew that such an operation required high-powered lamps which give off a significant amount of heat. The officers investigating the petitioner obtained a thermal imaging device and aimed it at the petitioner's residence. The Scan showed that the petitioner's house was substantially warmer than the neighboring units. Specifically, his garage, roof, and side of his house were extremely hot. Based on this thermal imaging information, the police obtained a search warrant for the residence. At trial the Petitioner moved to suppress the evidence from the thermal imaging device, but the court denied the motion. The Petitioner appealed to the 9th Circuit court which held that the petitioner had shown no subjective expectation of privacy (the first prong of the Katz test) as he had failed to even attempt to conceal the heat escaping from his home. The Petitioner appealed and the SCOTUS granted certiorari to answer the question of whether the use of a thermal imaging device operated from a public street aimed at a private residence constitutes a "search" within the definition of the Fourth Amendment (Kyllo v. United States, 2001).

Justice Scalia delivered the opinion of the Court on this case making three key points. First, Justice Scalia points to the pre-Katz doctrine of property rights being closely tied to the Fourth Amendment for the majority of the history of the United States stating "We have since decoupled violation of a person's Fourth Amendment rights from trespassory violation of his property, but the lawfulness of warrantless visual surveillance of a home has still been preserved"(Ibid). He goes on to argue in his second point that the privacy afforded to citizens by the Fourth Amendment would not be materially impacted by the rapid advance of technology. He reframes the question of the thermal imaging device to one about emergent technologies. "The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy" (Ibid). He then proceeds to point out that the guidance in Katz does not give effective guidance for this type of search. On one hand, a person has the right to be secure in their homes; however, as was pointed out at the circuit court, the Petitioner failed to even attempt to hide the heat coming from their home. Justice Scalia applied a new criterion on top of the existing Katz tests in order to assess whether the use of emergent technologies constitute a Fourth Amendment Search.

> While it may be difficult to refine Katz when the search of areas such as telephone booths, automobiles, or even the curtilage and uncovered portion of residences are at issue […] is a ready criterion with roots deep in the common law, of the minimal expectation of privacy exists, and that is acknowledged to be reasonable. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment. We think that obtaining by sense enhancing technology any information regarding the interior of the home

> that could not have been obtained without physical "intrusion into a constitutionally protected area" constitutes a search – at least where the technology in question is not in general public use (Ibid).

Therefore, on the grounds that the thermal imager in question was not widely available the public, the SCOTUS held that the use of the thermal imager was in fact a search under the Fourth Amendment. However, Justice Scalia had one final point to make.

Scalia and the Court recognized the potential danger of emergent technologies. The Government and dissent both heavily focused on the differentiation of "off the wall" observations and "through the wall" surveillance. They argued that this imaging did not detect the private activities in the home and as such was not a search. Justice Scalia soundly retorted his fellow justices and the Government's argument by once again quoting Katz. He points out that in Katz the eavesdropping device picked up the sound waves that reached the exterior of the booth. The government and dissent argued the reverse of the approach to Katz; that privacy ends at the edge of area being surveilled. Justice Scalia, in an effort to curtail future infringements of people's rights by technology, stated that simply reversing the logical flow of Katz is inherently illogical and "Would leave the homeowner at the mercy of advancing technology […] While the technology used in the present case was relatively crude, the rule we adopt must take account for more sophisticated systems that are already in use or development" (Ibid). Therefore, the SCOTUS reversed the Circuit Court's decision and applied a new criterion for emergent surveillance technologies.

The Final two cases in this framework were adjudicated by the current sitting SCOTUS, the Robert's Court. The Roberts court has continued the "culture wars" started by the Rehnquist

court and is as conservative if not more than the Rehnquist court. As Mendelson puts it "This is part of a decades-long turn toward textualist statutory interpretation in the Supreme Court" (Mendelson, 2018). meaning that instead of looking at the intent of statutes and the Constitution the court looks at a more literal reading of the statutes. The Roberts court exercises its power of judicial review, analysis on the constitutionality of federal and state laws, less than any other court in modern history (Whittington, 2014). Additionally, the Roberts Court has been faced with the difficulty of being the court responsible for ushering in the Internet age. This includes emergent technologies as are found in United States v. Jones litigation of GPS tracking, and the use of cell cite location data as found in Carpenter v. United States. Neither of these cases are considered cases of Judicial Review as they are litigations against the actions of the state, not the laws of a state.

The second case that deals with emergent technology is the United States v. Jones. This case is crucial to the development of this framework for two reasons. First, it deals with emergent technologies and further demonstrates that the Court tends to err on the side of caution when dealing with emergent technologies. Secondly, it expands on the opinion of Kyllo by officially reaffirming (post Katz) that the decision of Katz does not supplant the original understanding of privacy being tied to property rights, but expands the protections afforded by the Fourth Amendment. The standard in Katz is not the only standard by which Fourth Amendment question ought to be adjudicated but is a useful standard for Fourth Amendment question in both private and public arenas. This opinion, however, goes further and demonstrates that when the fundamental understanding of the Fourth Amendment being tied to property rights is violated, the Katz doctrine need not come into play.

In this case the Defendant, Jones, was suspected of trafficking narcotics. The FBI obtained a warrant authorizing the use of an electronic tracking device on the Jeep Grand Cherokee registered to Jones's wife. A warrant was issued, authorizing installation of the device in the District of Columbia and within 10 days. The FBI agents waited 11 days and installed a GPS tracking device on the undercarriage of the vehicle not in D.C., but in Maryland while the vehicle was parked. At trial, the Defendant moved to suppress the evidence obtained through the GPS device. The judge ruled to only suppress the data that was obtained while the vehicle was parked, but held that the remaining data collected was admissible due to the fact that people traveling in automobiles on public thoroughfares do not have a reasonable expectation of privacy. The circuit court reversed the conviction and denied the Government's petition for rehearing. The Government petitioned to the SCOTUS for a ruling and certiorari was granted to answer the question does attaching a GPS tracking device to an individual's vehicle and subsequent use of that device to monitor the vehicle's movement on public streets constitute a search within the context of the Fourth Amendment (United States v Jones, 2012)?

Again, Justice Scalia delivered the opinion of the Court making a critical point. Justice Scalia begins by pointing to the argument of the Government which first argued that the use of a GPS tracker was not a search based on the case of U.S. v. Knotts in which the Supreme Court previously found that a person traveling on the roadways does not have an automatic expectation of privacy. The Government uses this case to indicate that the defendant did not have a subjective expectation of privacy and thus does not rise to the standard set forth by the Katz Doctrine. Justice Scalia quickly dispatched this argument. He states that the Government's arguments are irrelevant citing the entire pre-Katz history of Fourth Amendment jurisprudence. "As explained for most of our history the Fourth Amendment was understood to embody a

particular concern for government trespass upon the areas it enumerates. Katz did not repudiate that understanding" (Ibid). What Justice Scalia does here is recognize that Katz did not replace the original formulation of Fourth Amendment protections, rather it expanded the protections therein. A person's property is still protected under the Fourth Amendment in a post-Katz world.

The effects of this opinion were twofold. First, validates the original understanding of the Fourth Amendment and asserts that the Katz doctrine is useful for developing a deeper understanding of Fourth Amendment protections; however, it does not supersede the protections afforded under the original interpretation by the addition of Katz. Additionally, by proxy, this case also made it so that any emergent listening device or tracking device that is used by the police whose operation requires entrance to or manipulation of private property is in itself a search regardless of the location of such property. Finally, this opinion granted that a person has an expectation of privacy with regard to their movements in totality. Any means of tracking a person's movement necessarily requires a warrant. This is critical as it will come into play in the final framework.

There is one final case that is necessary to review for the purposes of this framework. The case of Carpenter v. United States. For the purposes of this framework, this decision is the closest to a "case on point" that exists. This case provides an exemption of the third-party doctrine set forth in the previous cases of Smith and Miller. Further, it holds that warrantless access of cell phone records is a violation of the Fourth amendment. Finally, this case forces the SCOTUS to look at cases of emergent technologies with additional levels of scrutiny.

In this case, the FBI obtained the cell phone numbers of several robbery suspects, among them was the number of the Petitioner, Carpenter. Cell phones operate by connecting to the

nearest cell tower wherever that is. Whenever a user's cell phone connects to a new tower it generates a time-stamped record known as a cell site location information. Pursuant to the Stored Communications Act, the FBI compelled the cell carriers associated with Carpenter's numbers to divulge cell site location information (CSLI) data. This information lead to Carpenter's arrest and trial for robbery. At trial, the Petitioner filed a motion to suppress the evidence collected from the CSLI data, but the motion to suppress was denied. The Sixth Circuit Court of Appeals affirmed the trial court's decision holding that carpenter lacked a reasonable expectation of privacy in the CSLI as that information was already shared with the carriers and fell into the third party exception established in Smith and Miller. The SCOTUS granted certiorari to answer two questions. Does the Petitioner have a reasonable expectation of privacy in the location information collected by the FBI? Does carpenter's sharing of information with his wireless carriers fall into the third-party exception (Carpenter v. United States, 2018)?

Chief Justice Roberts delivered the opinion of the Court. He begins by acknowledging that the case presents some conflicts within the existing structure of Fourth Amendment Jurisprudence. On one hand, the case of U.S. v. Jones recognizes a person's privacy in their movements. The other issue is presented in the case of Miller, which indicates that information voluntarily turned over to third parties is not considered protected information. With this in mind, Justice Roberts reframed the question to analyze which one of these principals should win out. Justice Roberts makes two primary points to answer these questions. Initially, he points to the similarity of the facts between Jones and the current fact pattern. Similar to the GPS tracker used in Jones, the CSLI data used in this case was "Detailed, encyclopedic, and effortlessly compiled" (Ibid). He once again points out that the purpose of opinions like Jones is to recognize that individuals have a reasonable expectation of privacy in the whole of their physical movements, and goes on to

state that the uniqueness of the CSLI data is such that it does not fall under the Third Party doctrine. The Government's argument in this case relied heavily on the Third-Party Doctrine.

The Government argued that the CSLI data was similar to the data in Smith and Miller as it was controlled by a Third Party. In a dramatic departure from the conventional wisdom of the Third-Party Doctrine, Justice Robert's laid out his reasoning as to why this fact pattern was in fact not governed by the Third-Party Doctrine. He points back to Smith and Miller indicating that while they do establish the Third-Party Doctrine, the cases did not rely solely on the fact that the documentation was in the control of a third party. These cases also relied on the type of documents sought. In Miller, the documents seized by the government weren't considered private effects and papers partially because they were controlled by the banks, but also because they were business documents belonging to the banks in question. Additionally, in Smith the phone numbers that were called by Smith through the use of the Pen Register was not found to be unconstitutional because the nature of phone numbers is such that they are intended to be given out and not assumed to be private information. Again, in both Miller and Smith the SCOTUS not only took into consideration the controlling third party, but also the type of information that was communicated. Further, Justice Roberts argued that the information "shared" with the phone companies in this case are not voluntarily shared.

> The question we confront today is how to apply the Fourth Amendment to a new phenomenon: The ability to chronicle a person's past movements through the record of his cell phone signals […] the fact that the individual continuously reveals his location to his wireless carrier implicates the third-party principle of Smith and Miller […] We decline to extend Smith and Miller to cover these novel circumstances. Given the unique nature of cell

> phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection. Whether the Government employs its own surveillance technology as in Jones or leverages the technology of a wireless carrier, we can hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI (Ibid).

Based on this opinion, the SCOTUS held that the Government's acquisition from wireless carriers of the defendant's CSLI was a warrantless search and therefore protected under the Fourth Amendment. This affirmed the decision in Jones that an individual has a reasonable expectation of privacy with respect to their movements, and the fact that the government obtained the information from a third party did not overcome the Petitioner's Fourth Amendment rights. Further, the SCOTUS held that accessing information through the Stored Communications Act was not a permissible mechanism of accessing CSLI because the burden of proof on the Government to access information through this act does not rise to probable cause. Therefore, a warrant is necessary to obtain the CSLI data.

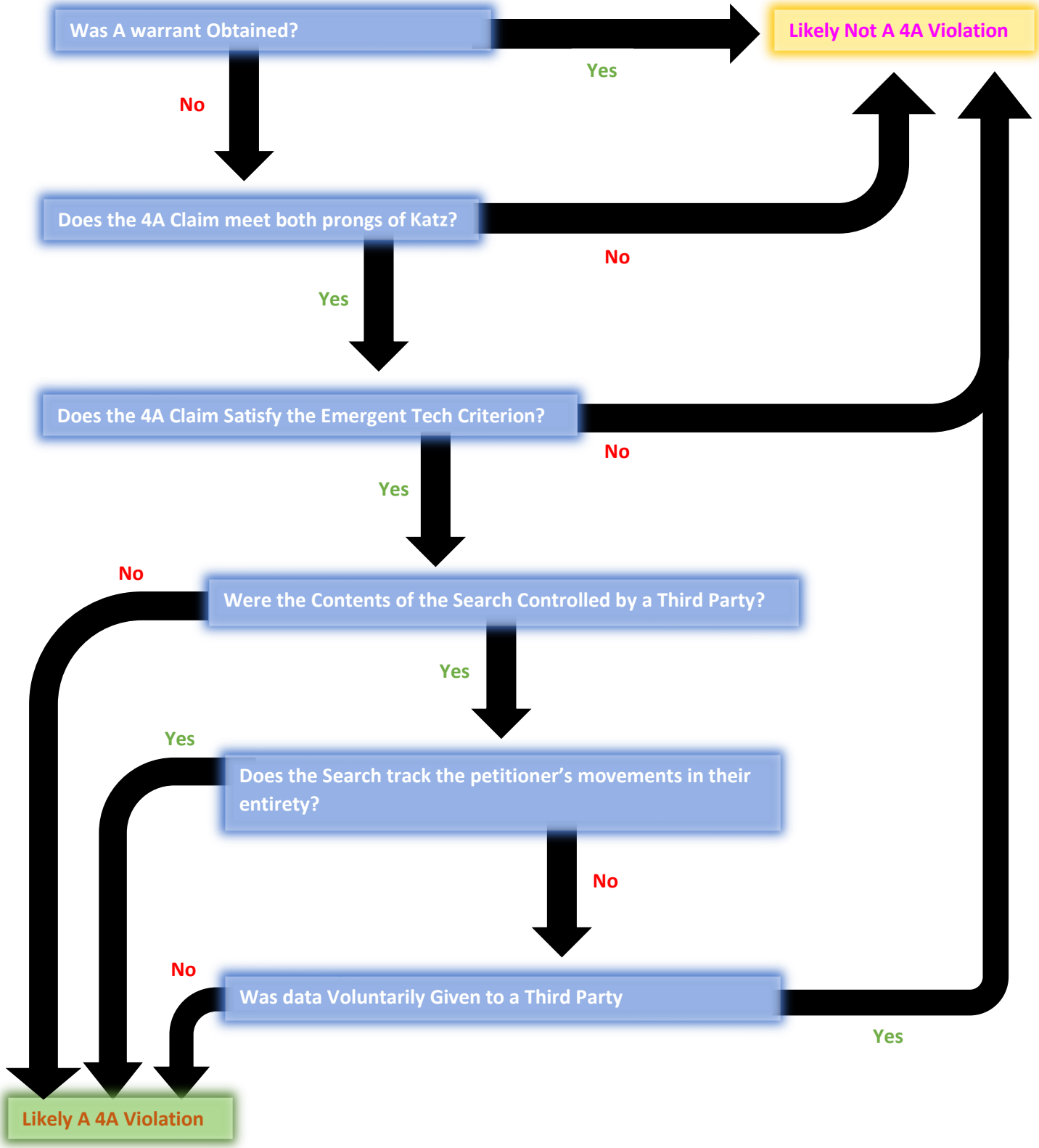
Now that these cases have been examined and their implications understood, it is possible to create the framework by which we can investigate the legality of DAPP. Before jumping into the framework, a review of the results of the case analysis is in order. The first three cases Wolf (1949), Irvine (1954), and Mapp (1961) established the classic pre-Katz view of the Fourth Amendment and the disposition of Fourth Amendment protections being tied exclusively to warrantless trespass within private property or effects. These three cases also demonstrate the process by which the Fourteenth Amendment's exclusionary doctrine was initially not applied to the Fourth Amendment, but in Mapp the understanding was changed, and the Fourth

Amendment now applies to both Federal and local authorities. In Katz (1967), the court added an additional test for Fourth Amendment claims known as the Katz Doctrine. This doctrine established that a person exercising their Fourth Amendment right must demonstrate a subjective expectation of privacy and that expectation of privacy must be one that society is willing to grant. Miller (1976) and Smith (1979) established the third-party exemption to the Fourth Amendment. These cases established that information freely given to third parties and/or under the control of third parties are not protected under the Fourth Amendment. Kyllo (2001), and Jones (2012) all deal with emergent technologies. Kyllo added an additional criterion beyond the typical Katz doctrine when assessing emergent technologies. The Kyllo doctrine adds the additional question to the two Katz test by asserting that in instances where technology is not readily available to the general populous, the use of said technology without a warrant is considered a search under the Fourth Amendment. Jones established that a person's movements, regardless of their visibility, are considered private and require a warrant to track that person's movements. Finally, Carpenter (2018) established recognized exceptions to the third-party doctrine, specifically with regard to instances where people are unable to choose whether to give their information to the government or not. Further, it established that data used to track people's movements is also protected under the Fourth Amendment.

While none of these cases directly address the use of data brokers or predictive policing, they do provide a basis to understand how the SCOTUS treat's the right to privacy and emergent technologies. This framework begins with the Katz doctrine. To be considered a Fourth Amendment violation either there needs to be some form of trespass into a person's constitutionally protected property by the police, or they must use the two-pronged test to demonstrate a "reasonable expectation of privacy." Since the predictive policing tools are a form

of emergent technology, on top of the Katz doctrine, we must establish whether the general public has access to the technology being used. If the public is unable to use the technology, then warrantless applications of any such technology will be considered a violation of the Fourth Amendment. Finally, since the data in question changes hands at least twice, the question of third-party possession of information comes into play. If the data given to the third party is not voluntarily given to the third party, or the data tracks the totality of an individual's movements, it would require a warrant. If all these conditions are met, then this would be considered a search under the Fourth Amendment and the information should be excluded at any ensuing trial, assuming the lack of a warrant.

Framework Flow Chart



Applying the Framework:

With this new understanding of the Fourth Amendment, it is possible to analyze the two models of DAPP put forth in Chapter 2. The first model we will analyze is the heat maps model that is widely used across the country. In this model, the police use historic crime data in order to determine when and where crime is most likely to occur. Some key facts about this system is that it doesn't specifically target any individuals. Due to the anti-circumvention arguments put forward by policing agencies, it is unclear whether the technology used in the construction of the heat maps are available to the public. With questions of the Fourth Amendment, there necessarily requires a crime and subsequent trial. For this reason, we will look at Andrejevic's example of the operationalization of the use of the heat maps model.

In this case, a police officer took his lunch in a parking lot where the model informed that a crime would likely take place. As he was finishing his lunch, he noticed two women breaking into cars. He apprehended them and they were arrested (Andrejevic, 2017). For the sake of this analyses, we will assume that they attempted to exercise their Fourth Amendment Rights.

First, we turn to the Katz doctrine to establish whether this is a violation of the Fourth Amendment. This case clearly does not fall into the understanding of the traditional expectation of privacy tied to public property because it clearly happened in neither of the defendant's homes or private property. The two women were out, in the middle of the day, in a parking lot accessible to the public while breaking into cars. It seems unlikely that they had a subjective expectation of privacy as required by Katz (Katz v. United States, 1967). Assuming however, that the two defendants were able to prove some subjective expectation of privacy, whatever privacy they assert would likely not be one that society is willing to grant. This is what legal

scholars refer to as a “prima facie” issue. Without this requirement, regardless of how sound the rest of the argument may be, the motion cannot go further. As such, none of the rest of the framework is needed. Predictive policing under this methodology is not a violation of the Fourth Amendment.

There are several other reasons as to why this model of DAPP does not violate the Fourth Amendment. While the data collected to generate the heat maps may be obtained from a data broker without the consent of the individual data is being taken from or without a proper warrant, the information did not technically lead to the arrest of these specific individuals. Essentially, the information data supplied by data broker’s may or may not have contained information identifying the two individuals. This information would not be discoverable at trial for several reasons, the primary of which is the anti-circumnavigation argument discussed earlier. Additionally, the defendant could very well not be aware of the existence of a DAPP in their area, so they might not even know to ask for this information during discovery.

As the Heat Maps model of DAPP quickly appears not to fall afoul of the Fourth Amendment, attention is turned to the SSL model of DAPP. Again, in this model, data is collected on subjects each of which is assigned a score between 1-500 with 500 being most likely to commit a crime. This model takes into consideration over 48 factors which include location information, proximity to crime, criminal history, etc. This model seeks to predict who will likely commit crimes in the future. It is operationalized in two primary ways. Police officers either give the suspected future perpetrator a “Custom Notification” or, when a crime is committed, bring in the “usual suspects” for interrogation. According to Asaro, “As a result, people on the list were far more likely to be detained and arrested by police, simply for being on the list.” (Asaro, 2019)

For this model, we look first at a case where the police suspect that a new narcotics dealer has moved into the area they patrol. They use the SSL to quickly compile a list of likely suspects and arrest them all for suspected trafficking. Using the SSL, they bring up the associated profile of the suspect and note that in prior communications he had made coded references to selling narcotics. Additionally, they note that this particular suspect was at or near the locations of several known drug deals. They obtain a warrant and search the suspect's house and find a large number of narcotics and narcotic paraphernalia. The suspect is arrested, but at trial assert's his Fourth Amendment right claiming it has been violated by the information obtained through the data brokers and sold to the police.

To analyze this Fourth Amendment challenge we once again turn first to Katz. Did the defendant have a subjective reasonable expectation of privacy? Depending on the court and judge, this could go either way, on one hand the defendant gave the information to control of third parties which further re-sold that information. It is fairly common knowledge that personal data is sourced through a multiplicity of different services; however, these services are necessary for activities of daily living, and will not function if you do not agree to these terms. In Carpenter v. United States, the SCOTUS determined that the third-party exception does not attach to information that was not voluntarily shared with a third party. Since the data collected and sold to data brokers is necessary for the function of devices such as computers and cell phones, this would fall into the third-party exemption established in Carpenter (Carpenter v. United States 2018). Given that the third-party exception to the Fourth Amendment doesn't apply in this situation, it can be concluded that the defendant asserting their Fourth Amendment right had a subjective expectation of privacy.

While the first branch of the Katz doctrine has been met, would this expectation of privacy be one that society as a whole is willing to grant the defendant? While this question cannot be definitively answered outside of court, there is a general discontent with the use of data brokers and the current state of data privacy. Many researches have critiqued the existence of data broker's as a violation of consumer protections and of privacy. In their article *The Limits of Transparency: Data Brokers and Commodification* Crain expresses "Many Americans are aware of commercial monitoring in a general sense and express desire for increased control over marketing data practices" (Crain, 2018). In Martin's article *The Unregulated Underground Market for Your Data: Providing Adequate Protections for Consumer Privacy in the Modern Era,* they indicate that there are several common concerns to the current state of data practices in society. "It [data collection] seems to be an invasion of consumer privacy. After all, in "real life," a regular person would not let a stranger follow them around the mall taking notes on their behavior and to report them back to some company they have never heard of. […] Another concern is related to the security practices of big data companies" (Martin, 2020). Therefore, the body of existing literature seems to affirm that society would be willing to grant a reasonable expectation of privacy when it comes to individuals. Therefore, both branches of the Katz Doctrine are satisfied.

Since DAPP is an emergent technology, we must also apply the emergent technology criterion defined in Kyllo v. United States. Kyllo established that beyond the Katz doctrine, when emergent technologies are used, the courts should turn and establish whether these technologies are available for public use when adjudicating them in the face of a Fourth Amendment claim (Kyllo v. Untied States, 2001). In this case, we have two emergent technologies we have the use of the SSL and the use of the data obtained through various means.

The data collection itself does not constitute a violation of the Fourth Amendment. The data was collected by a business and the Fourth Amendment does not protect people from businesses, but from the government. Therefore, we must look exclusively at the use of the SSL. While people on the list are informed of the existence of the list and their presence on it, it is not accessible or useable by the public (Asaro, 2019). As such, using the data purchased from the data brokers in order to use the SSL is not accessible for public use. The use of this data, therefore, constitutes a constitutional violation of the Fourth Amendment. This case meets the Katz doctrine and fulfills the additional criterion of emergent technologies. If the court were to find the exercise of the Fourth Amendment acceptable, the court would be forced to dismiss the case or overturn any conviction.

While the analysis thus far conducted is sufficient to demonstrate a violation of the Fourth Amendment, something interesting can be inferred from the way the SSL is operationalized. In the "usual suspects" model that we are testing, the police round up suspects which are near in proximity to the crime; however, this implies that the police have the location of these individuals at all times. In order to do this, the police must be tracking these individuals either through the data used in the SSL, or through other means. Either way, in order to determine if any of the "usual suspects" were within proximity of the crime when it happened, the police must be tracking the totality of their movements. If this is being conducted with a warrant on file, then this would be an acceptable use of police power. If the police do not have a warrant, then pursuant to the rationale in Jones and Carpenter, this would be an illegal search. While this doesn't fall specifically into our framework, it demonstrates how even the byproducts of the SSL can be tainted by Fourth Amendment violations. The exclusionary rule would attach and all the

fruits of searches because of the illegal action would be thrown out. In this case, that would be most of the evidence. As such, the defendant would likely go free.

While it is likely that simply based on the conclusions of president the SCOTUS would likely strike down the application of the SSL, the Robert's Court tends to shy away from questions of Judicial Review (Whittington, 2014). The application of an SSL in certain cities would likely mandate local and even state laws for its application. While the SSL program in Chicago had very little oversight or governance attached to it, other jurisdictions in the future very well may avoid that pitfall. Litigation to the SCOTUS level would likely be a case regarding judicial review, especially if it involved a class of people (those on the SSL). In this case, while the argumentation is likely sound, it is improbable that the Roberts Court would even hear such a case. SCOTUS Justices are lifetime appointments and Chief Justice Roberts is young at 65. Ingold's indicates in their article in Bloomberg that the average age of retirement is rapidly approaching 80 (Ingold, 2017). This means that Chief Justice Roberts will likely serve another 15 years. 15 years ago, Facebook was a year old, twitter was just an idea, and most of the services we rely on today were in their infancy or not even conceived of. If the SCOTUS does not touch these issues, what will happen in the next 15 years?

Chapter 5: Conclusions and Recommendations

The results of the legal analysis are mixed. It was expected that there would be some identifiable Fourth Amendment violations as both Asaro, and Martin point out there was virtually no oversight of data brokers or DAPP models. What was interesting was that there was no violation of the Fourth Amendment in the Heat Maps model. This finding is not necessarily all that surprising. In classical policing, it is common for police to identify areas of higher crime and dispatch more resources to those areas. DAPP heat maps only take this information and apply a statistical lens to them, which is not inherently violative of the constitution. While the use of data brokers in this area is concerning and warrants more research, it does not rise to the level of a constitutional violation.

Another interesting finding is that while the SCOTUS is normally a conservative body that moves incrementally, the SCOTUS seems to apply the Fourth Amendment fairly liberally. Two of the opinions on emergent technologies were written by Antonin Scalia, a famously conservative justice. The justices also recognize that the SCOTUS would likely not move quickly on adjudicating these matters, so they have implemented safeguards through many of the opinions discussed here in order to help protect the Fourth Amendment in light of a rapidly expanding surveillance infrastructure.

There are several continuing studies that I believe are necessary in this field of research. First, more work must be done on determining the efficacy of DAPP technologies. While there is much research critiquing these from a theoretical surveillance basis, there has been very little work done on the practical implications of these. For example, the SSL implemented in Chicago has very little information on efficacy, though a statistical analysis failed to reveal a statistically

significant impact to crime, there has been virtually no work done on the communities impacted by this type of DAPP (Asaro, 2019). Historically, police have targeted black communities and overpoliced these communities. It would not be particularly surprising if the SSL, whether intentionally or not, targeted minorities (Hinton, 2016). This kind of investigation would necessitate several years and a multiplicity of FOIA requests, and potentially lawsuits, in order to obtain the data. Another study that should be considered is on the specifics of how data purchased from data brokers are operationalized in both the SSL and Heat Maps models. Again, largely due to the anti-circumvention argument, this information is incredibly difficult to come by. This investigation would also necessitate FOIA requests, and potentially lawsuits to obtain the information.

For any policy makers, this research leads me to several policy recommendations. First, I would recommend against implementing a program like Chicago's SSL program. As has been demonstrated, this type of program is unconstitutional pursuant to the Fourth Amendment. It would be easier to determine a suspect and then use warrants and subpoenas to obtain the necessary evidence rather than attempt to shorthand justice with an SSL. While many municipalities are looking into the "heat maps" model, I cannot recommend the use of this model. While this may not rise to the level of a Constitutional Violation, these types of maps could be easily skewed by unjust laws and policies like those found in the eras of the war on poverty, the war on crime, and the war on drugs, and further intrench institutional racism. While the heat maps might help predict areas where crim is more likely to occur, as a means of crime prevention, it would likely be more useful to spend the municipalities resources on addressing the underlying issues causing the crime as opposed to attempting to respond to crime.

Works Cited

109th Congress (2006). Internet Data Brokers: Who has Access to your Private Records?. Serial No. 109-130.

Andrejevic, M. (2019). Automating Surveillance. *Surveillance & Society* 17(1/2) pp. 7-13.

Andrejevic, M (2017). To Preempt a Thief. *International Journal of Communications* Vol. 11 (2017) pp. 879-896.

Asaro, P. M. (2019). AI Ethics in Predictive Policing: From Models of Threat to Models of Care. *IEEE Technology & Society Magazine* June 2019 pp. 41-52.

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E (2019). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. *Pew Research*. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Bryden, D. P. (1992) Is the Rehnquist Court Conservative? *The Public Interest*, Fall 1992. pp. 73-88.

Cadwalladr, C. & Graham, E. H. (2018). Revealed 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach. *The Guardian.* https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Carpenter v. United States 138 S. CT 2206, 2018.

Crane, M. (2018). The Limits of Transparency Data Brokers and Commodification *New Media & Society* Vol. 20(1) 88-104.

Ferguson A. G. (2019) The Exclusionary Rule in the Age of Blue Data. *Vanderbilt Law Review* Vol 72:2:651 pp. 651-645.

Garrow, D. J. (2014) How Roe v Wade was Written. *Washington and Lee Law Review*, Vol. 71. No. 2. pp. 893-924.

Hinton, E (2016) – *From the War on Poverty to the War on Drugs: The Making of Mass Incarceration in America* Harvard University Press.

Ingold, D. (2017) Eighty is the New 70 as Supreme Court Justices Serve Longer and Longer *Bloomberg*. https://www.bloomberg.com/graphics/2017-supreme-court-justice-tenure/

Irvine v. California 347 U.S. 128, 1954.

Katz v. United States, 389 U.S. 347, 1967.

Kerr O. S. (2010) Applying the Fourth Amendment to the Internet: A general Approach. *Stanford Law Review*, Vol. 62 Iss. 4, pp. 1005-1049.

Kyllo v. United States 533 U.S. 27, 2001.

Lau T. (2020). Predictive Policing Explained. *Brennan Center for Justice*. https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained.

Letaru, K. (2018). The Data Brokers So Powerful Even Facebook Bought Their Data - But They Got Me Mildly Wrong. *Forbes*. https://www.forbes.com/sites/kalevleetaru/2018/04/05/the-

data-brokers-so-powerful-even-facebook-bought-their-data-but-they-got-me-wildly-wrong/#694634363107

Manes J. (2019) Secrecy & Evasion in Police Surveillance Technology *Berkeley Technology Law Journal* Vol. 34 pp. 503-565.

Mapp v. Ohio 367 U.S. 643, 1961

Martin, B. A. (2020) The Unregulated Underground Market for Your Data: Providing Adequate Protections for Consumer privacy in the Modern Era *Iowa Law Review* January 25, 2020 pp. 865-900.

McQuade, B. I. (2016). Police and the Post 9/11 Surveillance Surge: 'Technological Dramas' in 'The Bureaucratic Field. *Surveillance & Society* 14(1) pp. 1-19.

Menndelson, N. A. (2018) Change, Creation, and Unpredictability in Statutory Interpretation: Interpretive Canon Use in the Roberts Court's First Decade. *Michigan Law Review*, Vol. 117. pp. 71-142.

Moses, L. B. & Chan J. (2018). Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability. *Policing and Society* 28:7 pp. 806-822.

Neuborne, B. (2010) The Gravitational Pull of Race on the Warren Court. *The Supreme Court Review*, Vol. 2010, No. 1. Pp. 59-102.

Roser, M., Ritchie, H & E. Ortiz-Ospina (2020). Internet. *Our World In Data*. *https://ourworldindata.org/internet*

Smith, G. JD (2018). Data Doxa: The Affective Consequences of Data Practices. *Big Data & Society* January-June 2018 pp. 1-15.

Smith v. Maryland 442 U.S. 735, 1979.

United States Constitution. Fourth Amendment, Congress.Gov. https://constitution.congress.gov/browse/amendment-4/