The Fourth Amendment in the Digital World:

How Should Computers Be Searched With Respect to the Fourth Amendment?

Shivani Vikuntam

Barnard College, Columbia University

Information Science, Senior Thesis

Professor Steven Bellovin, Advisor

May 2016

I. Introduction

The United States' judicial system maintains the long held belief that one is innocent until proven guilty in a court of law. The Fourth Amendment is an incredible tool that exists to protect the citizens of the United States from unlawful searches and seizures, and grants them privacy from prying eyes and ears. The founding fathers felt it important enough to explicitly remind Americans that they have the right to feel safe and secure in their persons, houses, papers, and effects. The Fourth Amendment has been applied in a multitude of cases revolving around physical evidence. Recently, with the aid of technology, privacy has become more difficult to obtain. The emergence of digital data has created confusing and complicated new discourse as to how this necessary amendment should be applied and interpreted. When a cell phone is seized through a search warrant, just how much of the cellphone can be searched? What about a computer, or a hard drive? Just as this amendment had to be reconstructed when dealing with automobiles, it is time to reimagine how the Fourth Amendment applies to the digital world in order to protect the ever-growing user population.

I plan on approaching this topic by studying various court cases surrounding the Fourth Amendment, and using the various corresponding doctrines and precedents to argue that even though digital data is more compact than physical data, the Fourth Amendment still protects individuals from unlawful searches and seizures. The goal is to define and decide where the lines can be drawn during searches of digital data.

Today, information can be obtained instantaneously. We live in the information age where data has no bounds. Our access to data is also becoming infinite, as we have an

increasing amount of ways to "plug in". Our phones, computers, and even watches are able to access and store data. Social media has made it possible to be virtually connected to people all across the world with ease. With platforms like Facebook, Google, and Snapchat, the line between what's private and public is constantly being blurred and re-drawn. A single Facebook profile holds information like your full name, date of birth, gender, address, photos of you, and more. The Internet holds virtual versions of millions of us. With our technology advancing at an incredible rate, it's alarming that our laws are stagnant and not evolving.

Though our laws have not yet changed, there have been increasing conversations around how they should be applied to technology. Over the past few years, new technology has seamlessly eased into our lives, with the potential dangers and repercussions only becoming evident now. Computer searches are drastically different from physical searches of homes. A home, however big it is, can only hold so much information. It can only hold so many letters, books, and photos. A computer, on the other hand, can be compact while also having the capacity to hold terabytes of data. A terabyte is hard to fathom, so here are some quick facts: If all of the 17 million books and documents in the Library of Congress were digitized, they would take up 136 terabytes of information. A single terabyte can hold about 330,000 photos, 1000 hours of video, or 250,000 mp3 files (which would be about two years of continuous music).[1] All of this information can be stored on a small portable device, but very difficult to store in your house. This is why searching a computer is inherently very different from searching anything else—the access to an incredible amount of information.

---

[1] Rosberg, 2008
[2] Oxford English Dictionary

Consider the case of the terrorist owned Apple iPhone that was obtained after the San Bernadino terrorist attack. The FBI wanted to search the phone so they attempted to force Apple to create a backdoor to their encryption. This led to a national discussion around the idea of privacy and to what extent does the government have the right to access your personal information. With the ability to store large amounts of data, how *should* a computer be searched with respect to the Fourth Amendment? In order to protect what little privacy we have, the Fourth Amendment must be reevaluated when dealing with computer searches, as the protection offered should not only apply to tangible objects but also to information and data that can be digitally stored.

The Oxford English Dictionary defines "computer" as:

> An electronic device (or system of devices) which is used to store, manipulate, and communicate information, perform complex calculations, or control or regulate other devices or machines, and is capable of receiving information (data) and of processing it in accordance with variable procedural instructions (programs or software); *esp.* a small, self-contained one for individual use in the home or workplace, used esp. for handling text, images, music, and video, accessing and using the Internet, communicating with other people (e.g. by means of email), and playing games.[2]

Given this definition, it's accurate to consider that a computer qualifies as any data-storing device. This extends to smartphones, tablets, and even smart watches. When mentioning computers in this paper I will be referencing all of the qualifying devices as well.

[2] Oxford English Dictionary

The concept of privacy is most heavily protected under the Fourth Amendment. The Fourth Amendment reads: “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 persons or things to be searched.” [3]Past cases have depicted this right when it comes to searching homes and private property. However, this amendment has had to be reevaluated when dealing with new technologies before. Automobiles provide a demonstration of the Fourth Amendment extending beyond a physical home or building.

The concept of “know your rights” seems naive, but it’s incredibly important. Time and time again, individuals have demonstrated that they were not aware they had rights. Rights like that of an attorney being present during questioning, or the right to see a warrant before a search takes place. Media plays an important role here, as media often reaches a further audience than court case proceedings do. For example, Jay-Z’s song “99 Problems” featured a verse that alluded to a police encounter. The lyrics were a back and forth between Jay-Z and the police officer that pulled him over. The verse is:

> "Do you mind if I look round the car a little bit?
>
> Well my glove compartment is locked so is the trunk and the back
>
> And I know my rights so you gon' need a warrant for that”

The popularity of this song served to inform many young individuals of their rights, though Saint Louis University School of Law’s Professor Caleb Mason pointed out that there is no

[3] U.S. Const., amend. IV.

warrant requirement for car searches because cars are inherently mobile.[4] However, it is necessary for probable cause to be present.[5] With technology that allows us to store our personal data on everyday devices, it is important that we not just rely on mainstream media to educate us. The Fourth Amendment extends beyond personal property to include "papers" and "effects" and today it is fair to assume that computers fall under these categories.

[4] Carroll v. United States
[5] Mason, 2011

II. History & Origin

The creation of the Fourth Amendment originated from the negative experiences of colonists under the King. In order to enforce taxes and revenue laws, the "English authorities made use of writs of assistance", which were general warrants authorizing the bearer to enter any house or other place to search for and seize "prohibited and uncustomed" goods, and commanding all subjects to assist in these endeavors.[6] These writs of assistance were applicable not only for the remainder of the sovereign's life, but also for six additional months. These unreasonable timeframes and procedures offered colonists minimal protection from the crown. John Adams heard a patriot, James Otis, speak out against these writs of assistance in 1761, and later wrote, "[e]very man of a crowded audience appeared to me to go away, as I did, ready to take arms against writs of assistance." According to Adams, Otis's speech was "the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born."[7]

It's necessary to draw comparisons between the types of information that could have been searched for and seized in the 1700s and the type of information we own today. Though the containers of the information have changed drastically, the content has not. In the court case Riley V California, Justice Roberts noted that "the fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."[8] Keeping this idea in

[6] Justia Law
[7] 10 Works of John Adams
[8] Riley v. California

mind, it's fair to argue that the information stored in devices like our phones and computers need to be protected as strictly as information stored physically. The Fourth Amendment is centered on the idea of protection and privacy, and this needs to be restructured to fit our present day technological capabilities.

III. Existing Legal Background

There are several key court cases that help address the issues presented in this paper. These cases provide instrumental information and set important precedents in this area of law. The first of these cases is Riley v. California. In this case, the defendant David Leon Riley was pulled over for driving with expired license registration tags. After realizing Riley was also driving with a suspended driver's license, the police required the car to be impounded. It is procedure to perform an inventory search before the car is impounded to protect against potential liability claims and to discover hidden contraband. The search resulted in the discovery of two guns, which then led to Riley's arrest for the possession of firearms. At the time of arrest, Riley had his cell phone in his pocket, and it was collected due to the search incident to arrest principle. The police then searched the contents of the phone and found photos and videos associating Riley with a Gang, which led Riley to be linked with a gang related shooting that had occurred earlier that month. This link allowed Riley to then be charged for that crime, which included shooting at an occupied vehicle, attempted murder, and assault with a semi-automatic firearm. Riley attempted to suppress the evidence surrounding his gang association because it was required through his cell phone, however this motion was denied and a jury convicted Riley of all three counts. Riley was then handed a sentence of fifteen years to life in prison.[9]

Upon appeal, the United States Supreme Court faced an intriguing question that forced them to examine new technology through a constitutional lens: Was the evidence admitted at trial from Riley's cell phone discovered through a search that violated his

[9] Oyez, Riley v. California

Fourth Amendment right to be free from unreasonable searches? (*ibid*.) The answer is, yes. The detective who searched Riley's phone testified that he "went through" his phone "looking for evidence, because...gang members will often video themselves with guns or take pictures of themselves with guns."[10] This search could be equivalent to a detective entering a house belonging to someone who was found with marijuana and then proceeding to search for marijuana plants because sometimes people grow their own product. This is an incredibly broad interpretation of the extent to which a search incident to arrest can be applied.

The Fourth Amendment was created with the technology of the 1700s in mind. The founding fathers could not have predicted the rise of the technological age and the progress we would have been able to make in such a short period of time. However, the industrial revolution brought about new technologies such as the car, which introduced new places that could be searched. The next case that changed the way the Fourth Amendment was applied was Carroll v. United States. This 1925 case was the first to address how searches and warrants would need to be applied to automobiles. This case originated from the National Prohibition Act, which was passed to enforce the Eighteenth Amendment that effectively prohibited the manufacture, sale, or transportation of alcohol. The National Prohibition Act not only enforced the Eighteenth Amendment, but also stated, "No search warrant shall issue to search any private dwelling occupied as such unless it is being used for the unlawful sale of intoxicating liquor, or unless it is in part used for some business

[10] Riley v. California

purpose such as a store, shop, saloon, restaurant, hotel, or boarding house."[11] The Act continued by stating

> "When the commissioner, his assistants, inspectors, or any officer of the law shall discover any person in the act of transporting in violation of the law, intoxicating liquors in any wagon, buggy, automobile, water or air craft, or other vehicle, it shall be his duty to seize any and all intoxicating liquors found therein being transported contrary to law. Whenever intoxicating liquors transported or possessed illegally shall be seized by an officer he shall take possession of the vehicle and team or automobile, boat, air or water craft, or any other conveyance, and shall arrest any person in charge thereof." (*ibid.*)

Additionally, the twenty-fourth section of the Act of 1789, which was created to regulate the collection of Duties, states:

> "That every collector, naval officer and surveyor, or other person specially appointed by either of them for that purpose, shall have full power and authority, to enter any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed; and therein to search for, seize, and secure any such goods, wares or merchandise; and if they shall have cause to suspect a concealment thereof, in any particular dwelling house, store, building, or other place, they or either of them shall, upon application on oath or affirmation to any justice of the peace, be entitled to a warrant to enter such house, store, or other place (in

[11] Carroll v. United States

> the daytime only) and there to search for such goods, and if any shall be found, to seize and secure the same for trial; and all such goods, wares and merchandise, on which the duties shall not have been paid or secured, shall be forfeited."[12]

Carroll v. United States brought forth a myriad of issues surrounding the many acts that were created in order to avoid the Fourth Amendment so that the Eighteenth Amendment could be better enforced. The Court found that there is a distinction between goods being concealed in a dwelling house or similar place, versus goods concealed in a movable vessel where "they could readily be put out of reach of a search warrant." (*ibid*.) The Court pointed out that it would be unreasonable for the officer of law to be authorized to stop and check every single passing automobile on the chance that they might find prohibited alcohol, which would "subject all persons lawfully using the highways to the inconvenience and indignity of such a search." (*ibid.*) The Court concluded that for those lawfully within the country who are also entitled to use public highways, have a "right to free passage without interruption or search unless there is known to a competent official, authorized to search, probable cause for believing that their vehicles are carrying contraband or illegal merchandise." (*ibid*.)

The conclusion of Carroll v. United States is important because it introduces automobiles into the world of the Fourth Amendment. Despite being movable, the Court clarified that probable cause is still necessary for a search to take place. This set the precedent that added to the furthering away of warrantless or unreasonable searches. This decision announced that the Court was not in favor or searches of any kind that happened

[12] Carroll v. United States

without probable cause. Incidentally, this decision strengthened the argument that privacy is also a fundamental right that needs to be protected.

The case Katz v. United States was another monumental Fourth Amendment decision. Federal agents suspected Katz was transmitting gambling information to his clients in other states over the phone. The agents attached an eavesdropping device to the outside of a public telephone booth that was commonly used by Katz. Based on the recordings of his conversations, Katz was convicted under an eight-count indictment for the illegal transmission of wagering information from Los Angeles to Boston and Miami. The United States Supreme Court was tasked with answering the following question: Does the Fourth Amendment protection against unreasonable searches and seizures require the police to obtain a search warrant in order to wiretap a public pay phone? In a 7-1 decision, the court answered yes, a search warrant is required.

Katz v. United States offers some unique new aspects to the Fourth Amendment. Key details of this case include the telephone that was used being available to and located in the public, and that individuals had to pay to use it. Additionally, the pay phone was in an enclosed space that offered the customer privacy from the outdoors. The Court set about answering two key questions: 1) Is a public telephone booth a constitutionally protected area? 2) Is the physical penetration of a constitutionally protected area necessary before a search and seizure can be said to violate the Fourth Amendment? Justice Stewart delivered the opinion of the Court, and pointed out that searching for a "constitutionally protected area" detracted from the key issue. Justice Stewart explained that the Fourth Amendment serves to protect people, not places. He further explained that, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment

protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[13]

The government attempted to argue that the phone booth was constructed of glass, which prevented any privacy. However Justice Stewart pointed out that Katz sought to exclude the uninvited ear, not the intruding eye. Justice Stewart stated that, "One who occupies it [the telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication." (*ibid.*) For the concurring opinion, Justice Harlan stated that, "The point is not that the booth is 'accessible to the public' at other times… but that it is a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable."(*ibid.)* Justice Black wrote the dissenting opinion and argued that the founding fathers would have taken the concept of eavesdropping into consideration when writing the Fourth Amendment. He concluded that the Fourth Amendment does not apply to eavesdropping.

Given the changes in technology, the concept of eavesdropping has evolved greatly. What once required physical proximity now has infinite boundaries. I would argue that the founding fathers did not imagine a time in when communication is as instantaneous as it is today, and therefore could never have predicted the evolution of eavesdropping.

Another important case to draw from is Kyllo v. United States. This is a groundbreaking case as it was one of the first times the United States Supreme Court

[13] Katz v. United States

touched on new technological advances and how they might alter the way in which searches and seizures are conducted. The case begins with a Department of the Interior agent suspecting Danny Kyllo of growing marijuana. The agent used a thermal-imaging device to scan his residence, which allowed the agent to see if the amount of heat emanating from the home was consistent with the high-intensity lamps generally used for indoor marijuana growth.[14] The imaging revealed hot spots within the home, and along with informants, and utility bills, a federal magistrate judge issued a warrant to search Kyllo's home. The search resulted in the finding of marijuana plants and Kyllo was arrested. Though Kyllo argued that the use of thermal imaging violated his right to privacy in his home, the Court of Appeals held that he did not attempt to hide the heat escaping from his home, and the imager "did not expose any intimate details of Kyllo's life". (*ibid.)* The question that was brought forth to the United States Supreme Court was the following: Does the use of a thermal-imaging device to detect relative amounts of heat emanating from a private home constitute an unconstitutional search in violation of the Fourth Amendment?

In a 5-4 decision, the Court held that the search was unconstitutional. The Court stated that at the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.[15] The thermal imaging device, called the Agema Thermovision 210, detects infrared radiation and operates like a video camera showing heat images. However, a line must be drawn between what is reasonable and what exceeds entry into the house. The thermal imaging device is not something that is generally used by the public, and therefore it is not reasonable to

[14] Oyez, Kyllo v. United States
[15] Kyllo v. United States

assume that individuals can secede that right to that specific type of privacy. The Court held that, "where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." (*ibid.)* This conclusion is important because it highlights new technology as something that is not yet in general public use. However, technology such as this thermal imaging device may become more readily available to the public in the future. Homes are more strongly protected by the Fourth Amendment than anything else. Technology is advancing at an incredible rate, while also becoming more accessible. Because of this, the courts should maintain that, regardless of the availability or accessibility of the technology in question, invasion of privacy beyond what can be perceived with human senses is unreasonable. For example, binoculars are enhancing human eyesight, whereas infrared cameras are going beyond what humans are capable of doing independently.

The case of United States v. Comprehensive Drug Testing investigated whether broad blanket type searches and seizures were constitutional. This case involved many players and is incredibly intricate. The case began in 2002 when the federal government began investigating the Bay Area Lab Cooperative (BALCO), which it suspected of providing steroids to professional baseball players. It also happened that that year the Major League Baseball Players Association also entered into an agreement with the Major League Baseball, "providing for suspicionless drug testing of all players".[16] As part of the agreement, urine samples were to be collected during the first year, and they would be tested for banned substances including steroids. It's important to note that the players

[16] U.S. v. Comprehensive Drug Testing

were assured that the results would remain anonymous and confidential. This program was administered by an independent business, called Comprehensive Drug Testing, Inc., although the actual tests were performed by Quest Diagnostics, Inc. Comprehensive Drug Testing did however maintain a list of the players and their respective test results.

Now, back to the investigation the federal government was involved with: the BALCO investigation. During this investigation, the federal government learned of ten baseball players that had tested positive in the CDT program. The government then secured a grand jury subpoena in the Northern District of California seeking all "drug testing records and specimens" pertaining to Major League Baseball in CDT's possession. CDT responded by attempting to file a motion to quash the subpoena. But the government had then obtained a warrant in the Central District of California authorizing the search of CDT's facilities in Long Beach. The warrant was limited to the records of the ten players that the government had probable cause for, but when the warrant was being executed the government seized and reviewed the drug testing records for hundreds of players in Major League Baseball.[17] Now, CDT had the drug testing records, but the actual specimens were kept at Quest Diagnostics. Because of that, the government obtained a warrant from the District of Nevada for the urine samples. The government also obtained additional warrants for records at CDT's facilities in Long Beach and Quest's facilities in Las Vegas. And finally, the government served CDT and Quest with new subpoenas demanding production of the records it had just seized. (*ibid.*)

The Central District of California found that the government acted beyond the scope of the warrant and ordered that the property be returned. This order is referred to as the

[17] U.S. v. Comprehensive Drug Testing

Cooper Order, named after the presiding judge, Judge Cooper. However, the government didn't just stop there. The warrant the government received explicitly required that "computer personnel" conduct the initial review of the seized data, and be responsible for segregating materials that were not the object of the warrant so that they could be returned to their owner. Judge Cooper found that this had been entirely ignored and a case agent had sifted out information pertaining to all professional baseball players, and used that information as probable cause to then gain access to additional warrants and subpoenas. If this sounds illegal and unconstitutional to you, you're not the only one who thinks so. Another judge, Judge Illston found, "no forensic lab analysis, no defusing of booby traps, no decryption, no cracking of passwords and certainly no effort by a dedicated computer specialist to separate data for which the government had probable cause from everything else in the Tracey Directory."[18] Here, you have an instance of the federal government blatantly violating a warrant. The Court reflected this by stating, "it was wholly unnecessary for the case agent to view any data for which the government did not already have probable cause because there was an agent at the scene who was specially trained in computer forensics." (*ibid.*) It was also noted that, "Judge Cooper found that the government utterly failed to follow the warrant's protocol. Judge Illston also found that the government's seizure, in callous disregard of the Fourth Amendment, reached information clearly not covered by a warrant." (*ibid.*) So here, you have a situation in which the federal government purposefully violated the Fourth Amendment in order to get its hands on information as to which it lacked probable cause. (*ibid.*) The government's defense was that they happened upon the information accidentally, and that the discovery fell under the

[18] U.S. v. Comprehensive Drug Testing

plain view exception. However, the plain view exception cannot be applied when the case agent looked through all of the data, and the information was not accidentally and unintentionally discovered.

The case resulted in the Ninth Circuit deciding en banc that the government had, "violated the Fourth Amendment rights of the parties when it conducted an overbroad seizure of electronic drug testing records of Major League Baseball players." (*ibid.*) This decision set an important precedent as it highlighted two main issues: the specificity of warrants and the need for a third party to handle the segregation of data as digital data can be immense.

Another landmark Fourth Amendment case was United States v. Jones. In 2004, Antoine Jones, owner and operator of a nightclub in the District of Columbia, came under suspicion of trafficking in narcotics and was made the target of an investigation by a joint FBI and Metropolitan Police Department task force. The police investigated Jones by surveying the nightclub, installing cameras focused on the club, and installing a pen register and a wiretap covering Jones's cell phone. In 2005, Antoine Jones was arrested for drug possession after police had attached a GPS tracker to his car. The police used the tracker to monitor his movements for a month without judicial approval. The United States Supreme Court was faced with the following question: did the warrantless use of a tracking device on Jones's vehicle to monitor its movements on public streets violate Jones's Fourth Amendment rights?[19] In a unanimous decision, the Court ruled: yes--this was a violation of the Fourth Amendment. Justice Scalia noted that the case resolved into a singular issue: whether the attachment of a Global-Positioning-System (GPS) tracking device to an

[19] Oyez, United States v. Jones

individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets, constitutes a search or seizure within the meaning of the Fourth Amendment.[20]

The Government applied to the United States District Court for the District of Columbia for a warrant authorizing the use of an electronic tracking device on a car registered to Jones's wife. The warrant was issued, however it authorized installation of the device in the District of Columbia within ten days. Agents installed the GPS tracking device eleven days later and in Maryland, blatantly violating two terms of the warrant. Over a four-week period, the device relayed over two thousand pages of data. (*ibid.*) In the Court's opinion, Justice Scalia drew back to the intentions of the founding fathers and stated, "It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." (*ibid.*)

In a concurring opinion, Justice Alito analyzed the case by asking whether the respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove. Justice Alito further discusses the role of technology in this case and states, "New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile...On the other hand, concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions. This is what ultimately happened with respect to wiretapping." (*ibid.*) Justice Alito also explained how in the pre-

[20] United States v. Jones

computer age, traditional surveillance was not discreet and was incredibly difficult and costly. Justice Alito pointed out that, "the surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance. Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources." (*ibid.*) When considering it from that angle, a simple drug possession charge is not enough to merit such a search. Again, this case came down to whether the monitoring of an individual accords with expectations of privacy that our society has recognized as reasonable. Despite our technological advances with GPS tracking and location services, society has still not willingly given up on the right to and expectation of privacy.

These six cases together lay the foundation for the argument that in order to protect what little privacy we have, the Fourth Amendment must be reevaluated when dealing with computer searches, as the protection offered should not only apply to tangible objects but should also extend to information that can be stored.

IV. Search Warrants

Search warrants inevitably bring up the issue of legal process, which I will not be addressing in this thesis. However, I will be arguing what the outcome *should* be, and not how it should reach there. That, I'll leave to the lawyers. In terms of search warrants, I will be addressing the specifications and details through the following sections: explicitness, scope, time, and third party searches and analyses.

Explicitness

According to the Fourth Amendment, issued warrants must describe the place to be searched and the persons or things to be seized. Computers are a bit more complicated since information is located within the hardware. When dealing with searching computers, search warrants must be explicit in exactly what they are searching for with reference to content and file/data types. Anything beyond that scope would constitute an illegal search. As previously mentioned, computers can store *a lot* of data. Because of this, when searching for something in particular, say a certain picture, you need to know what to search for. If you're searching for a photo of a dog, you should search for the name at the very least. If you go in blindly with only an idea of what you're looking for, you will essentially be searching for a needle in a haystack. However, in this scenario, the haystack would be your computer, and the government would be examining every piece of straw to see if it matches what it might be looking for. And if they happen to find something that isn't legal, then they

must act on it as well. It is unfair and unreasonable to allow for a blanket warrant be issued for a computer given the massive amount of data a computer can store.

Instead, the warrant needs to specify what it is looking for before the search and seizure takes place. Orin Kerr, a professor of law at the George Washington University School of Law argues heavily that limitations and authorizations need to occur in ex post review in order to set the results in the proper manner. He states, "Ex post review provides the standard method for developing the case law of the reasonableness of searches executed pursuant to warrants. The government executes the warrant first. Then, when charges are filed, a defendant will move to suppress the evidence discovered. The court will hold a hearing about precisely how the warrant was executed, and will then issue an opinion as to whether the method of execution was reasonable."[21] However, I would argue that this sets a dangerous precedent given the sheer amount of data that can be readily available in a computer. Allowing too many cases where they realize the error "in retrospect" is dangerous and undermines the right to privacy and unreasonable searches that the Fourth Amendment guarantees.

In addition to placing restrictions before the warrant is executed, I also argue that the warrant must be explicit in categories of content. In terms of particularity, the warrant needs to specify whether the search is being conducted on the physical computer or the information that is stored within the computer. In Riley v. California, Chief Justice Roberts alludes to a phone's data being safe, though a razor blade hidden in the phone case could pose a threat. Under that line of thought, contraband could be hidden within the physical components of a computer. It is unreasonable to not distinguish between the physical data

[21] Kerr, 2010

and physical computer. If a warrant were for the search of the physical computer, it would go beyond the scope of said warrant to search the digital data within the computer. Therefore, when issuing a warrant for the search of a computer, a distinction between the physical computer and the digital data needs to be apparent.

If the warrant is for the search of the digital information stored within a computer, the warrant must specify exactly what it is looking for in terms of files and content. For example, "illegally downloaded music" is not sufficient. The warrant needs to explicitly state what file types it is looking for. Computers are clever, and often times, file types in terms of extensions are not what they appear. A photo that is of PNG file type can simply change its extension so that it appears as an XLS, or Excel spreadsheet file type. If a warrant were to search for child pornography, it would not search through spreadsheets, and would then miss this file. In order to combat this, the actual file type needs to be determined through the file command, or equivalent, for pattern matches. The file command is a standard Unix program that recognizes the type of data contained in a computer file. This is a beneficial check because it can comb through the data and not expose the contents of the data to anyone. The file command can only tell you what the file looks like in terms of what kind of data it contains (photos, PDFs), but it does not tell you what the content is. This ensures that a reasonable search occurs, and the owner's privacy (in terms of data that doesn't pertain to the case) is not violated.

Scope

The scope of the search warrant needs to be specified before the warrant is executed. The restrictions and scope must be identified and stated before any searching

takes place. I argue that ex-ante restrictions are necessary to maintain the integrity, intentions, and purpose of the Fourth Amendment. In order to limit the amount of information outside the warrant comes into plain view, unlike what happened in United States v. Comprehensive Drug Testing, it is important to impose limits on how computers are searched. This is a practice that has been done in the past, and must become a necessity for search warrants pertaining to digital data. Orin Kerr discusses this, and provides an example of when ex-ante restrictions were used. He states,

> "In *In the Matter of the Search of: 3817 W. West End*, the government applied for a warrant to search a suspect's home and seize her computers to search them for evidence of tax fraud. The magistrate judge signed the warrant, but placed a condition on the warrant forbidding the government to search any seized computers until the government had proposed and the magistrate had accepted a search protocol. The government seized a Hewlett-Packard computer and a number of computer disks, and then met with the magistrate judge to discuss the search protocol. The government argued that the judge lacked any authority to restrict the government's search of the seized computer, but the magistrate concluded that such a protocol was necessary to ensure that the warrant was executed in a reasonable way. The judge then gave the government twenty-one days to submit a search protocol, with the warning that if the government did not do so it would have to return the computer unsearched."[22]

[22] Kerr, 2010

This is an excellent example of the types of reasonable restrictions that should be put in place. When reviewing the case of United States v. Comprehensive Drug Testing, it became apparent that the warrant was executed in an unreasonable manner. The government went beyond the scope that was originally stated and intended. The case of United States v. Comprehensive Drug Testing set a precedent that broad blanket type searches and seizures were not constitutional. The Cooper Order specifically ordered that the property and records containing the drug testing records be returned to the rightful owners. Additionally, reasonable restrictions are necessary in order to uphold the probable cause necessity. In the United States v. Comprehensive Drug Testing case, it was clear that the government disregarded the Fourth Amendment and accede information not covered by the warrant, in order to bypass the lack of probable cause. Without these restrictions, an individual is completely vulnerable, as it's been stated by the United States Supreme Court that our computers today hold massive amounts of personal data.

In the case of United States v. Comprehensive Drug Testing, Orin Kerr points out that, "according to the en banc court, magistrate judges should impose a series of conditions on computer search warrants to ensure that the government does not overreach and find evidence outside the scope of the warrant." (*ibid.*) Orin Kerr argues that these restrictions need to be discovered upon review of a case, however the reason that these restrictions be put into place ex-ante is computers are a form of technology that is completely new to the Fourth Amendment era. A single computer can hold the information found in a thousand houses and thousands of more file cabinets. Because of this, the warrant must provide some framework or else the search becomes unreasonable.

Additionally, the Vermont Supreme Court recently issued a decision on the issue of whether magistrate judges have the discretion to attach ex ante or prospective conditions to a search warrant. The court concluded that ex ante search restrictions are "sometimes acceptable". In a 2012 blog post, Orin Kerr writes, "in the court's view, the warrant clause of the Fourth Amendment is not just about establishing probable cause and particularity. Rather, warrants are designed to minimize privacy invasions by making sure that "investigatory promise" of a search justifies the resulting "collateral exposure" in that particular case."[23] Kerr continued to state that the Vermont court allowed the Magistrate judge to decide the level of restrictions based on how invasive the warrant is. Kerr phrased it well when he summarized that "ex ante restrictions are 'sometimes' permitted as ways of regulating the process to try to protect privacy in light of the 'interplay' between probable cause, particularity, and reasonableness." (*ibid.*) Though this is an appellate decision, the use of ex ante restrictions should be applied to all search warrants pertaining to computers and digital data.

Time

The search warrant should specify a time limit for how long a computer can remain in the court's possession. This should not be repealed or retroactively altered. This would mean that the court has a set amount of time to search through the computer to find what they are searching for. If anything is unable to be produced within that time frame, the computer is to be returned to the owner. Absent explicit permission from court, a search

[23] Kerr, 2012

that goes beyond a certain amount of time is unreasonable. Orin Kerr gives an example of this requirement in action with the case of United States v. Brunette. In this case, a magistrate judge issued a warrant to search computers with the stipulation that the forensic analysis of the computers had to be conducted within thirty days of the physical search. This established a two-step process: physical search, then forensic analysis. The physical search was completed within five days, and the agents applied for and received an extension from the magistrate judge giving them an additional thirty days to search the computers. One of the computers was searched within the new extended period and revealed images of child pornography. The second computer was searched outside of the extended period and also revealed images of child pornography. The court ruled, "the images discovered in the renewed thirty-day window were admissible, but that the images discovered on the second computer searched after the time had expired had to be suppressed based on the government's failure "to adhere to the requirements of the search warrant and subsequent order."[24]

Establishing a reasonable time frame is something that can be assessed by the respective judge given the situation. If the warrant is for a large amount of data, then the time can be extended. However, it is unreasonable to have an unlimited time to search through data. This is mainly due to the Sixth Amendment, which guarantees the right to a speedy and public trial. Imagine if the government had a warrant to search a home for the presence of illegal firearms. It wouldn't make sense for them to search through computers or hard drives because it would be impossible to find physical firearms in digital data. Additionally, it wouldn't make sense for the government to be allowed an unlimited time to

[24] Kerr, 2010

search through the entire house. Time restrictions are necessary because the search warrants aren't being executed on someone that has already been found guilty. Since the individual has not been tried yet, and only evidence is being collected, it is inherently unfair and unreasonable to allow their personal and private property to be searched for an unlimited or unreasonable long period of time. The trial must commence at some point. Additionally, reasonable time restrictions will also ensure efficiency during searches.

In United States v. Mutschelknaus, the magistrate judge imposed a requirement that the search of seized computers must occur within sixty days of the initial seizure. The defendant moved to suppress the evidence found on the computers, claiming the sixty days was unreasonable and that it violated Rule 41e2A of the Federal Rules of Criminal Procedure, which requires the execution of a warrant within ten days. However, the Eighth Circuit disagreed, and noted that the agents had been able to search the computer within the stipulated sixty-day period. Additionally, the Government contended that Rule 41e2A of the Federal Rules of Criminal Procedure only requires that the search warrant be executed within ten days and does not require the subsequent examination of the items seized to take place within ten days.[25] In this case, I agree with the ruling from the magistrate judge, as the judge had set the time period based on the warrant that was brought forth. Additionally, the time it takes to seize items is not necessarily the same as the time it would take to examine the seized items. Because of this, it makes sense to set separate reasonable time limits for executing the search and then for examining the seized materials. And as more cases come forth, the courts will be able to obtain a better idea of standard time

[25] Leagle, 2015

duration for the search warrant. Thus they can work to make the time limit as reasonable as possible without ignoring people's rights or obstructing justice.

Third Party Searches and Analysis

The purpose of a search is to discover something that already exists. In order to create a fair trial, there cannot be a bias within the search procedure. All searches of computers and the analysis on the data must be conducted by a third-party in order to avoid bias. This must be a requirement in all warrants involving computers. In United States v. Comprehensive Drug Testing, one of the stipulations of the warrant was that "computer personnel" conduct the initial review of the seized data and were to be responsible for segregating the materials not the object of the warrant for return to their owner. Without this stipulation, all of the contents would fall under the plain view doctrine if the case agent was the one to sift through all of the data. In this case, the government argued that it didn't violate protocol because, "the warrant didn't specify that *only* computer personnel could examine the seized files, and the case agent was therefore entitled to view them alongside the computer specialist."[26] This argument is weak at best. However, in order to avoid this type of obtuse argument, I argue that search warrants pertaining to computers explicitly specify that *only* computer personnel or the third party be allowed to examine the seized data.

Orin Kerr also discusses the idea of third party searches in his paper *Ex Ante Regulation of Computer Search and Seizure*. He states,

[26] U.S. v. Comprehensive Drug Testing

> "Magistrate judges must require that case agents cannot conduct the electronic search themselves and must never learn of any evidence discovered outside the warrant during the electronic search.[82] The computer forensic analysis must be performed either by computer specialists who are not on the case or a non-government third party hired to conduct the analysis.[83] In either event, the case agents with primary responsibility for bringing criminal charges must be walled off from any evidence outside the warrant's scope."[27]

I agree with the stipulation noted above--it is imperative that the seized data not be exposed to any bias, and that the evidence and the warrant function dependently in the justice system. If the entirety of the seized data were exposed to individuals who were biased and were searching for illegal activity, then they would have an incentive to look through all of the data, thus rendering the by chance nature of the plain view doctrine null. Additionally, the way in which the computer is searched is important. Software that searches for specific triggers (i.e. what is explicitly mentioned in the warrant) should be used, rather than software that uses blanket searches that searches for anything that is illegal.

Search warrants are complicated tools that have immense power. In order to use this tool appropriately when dealing with computers to avoid violating the Fourth Amendment, ex ante restrictions must be applied, the scope must be outlined, reasonable time limits for the search and analysis must be placed, copies of the data must be made, and it must be mandated that the searches and analysis be conducted by third party personnel.

[27] Kerr, 2010

V. Search Incident to Arrest

Riley brought forward the realization that today our phones are almost always on us. In the opinion for the unanimous court, Chief Justice Roberts wrote that modern cell phones are, "now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[28] Additionally, according to one poll, nearly three-quarters of smartphone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower. (*ibid.*) So on the off chance we are arrested, our phone is most likely going to be taken as well. So why do the police have the right to take our phone if we've been arrested? The case, Chimel v. California (1969) lays some of the current groundwork for the search incident to arrest principle. Chimel was arrested within his home, and the police officers proceeded to search his entire three-bedroom house, and even went so far as searching through the contents of drawers. Due to the broad search that resulted from a mere arrest, the Court created the following stipulation and clarification for assessing the reasonableness of a search incident to arrest:

> "When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer's safety might well be endangered, and the arrest itself frustrated. In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its

[28] Riley v. California

> concealment or destruction. . . . There is ample justification, therefore, for a search of the arrestee's person and the area 'within his immediate control'—construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence."[29]

This provides a very reasonable explanation to the search incident to arrest principle. If someone was arrested and had a weapon on him or herself, they could harm someone. Additionally, having contraband on oneself is probable cause.

Chimel v. California set the framework for the search incident to arrest principle; several other cases added the additional structure. In 1973, United States v. Robinson applied the "Chimel analysis" in the context of a search of the arrestee's person. Robinson was arrested for driving with a revoked license, and during the routine pat down search, the police officer felt, "an object that he could not identify in Robinson's coat pocket".[30] The object was a crumpled cigarette package. The office opened the package and found fourteen capsules of heroin. Based on Chimel v. California, the Court of Appeals concluded that this search was unreasonable because they felt that opening a cigarette package "could not be justified as part of a protective search for weapons". (*ibid.*) However, the United States Supreme Court reversed this decision and deemed the search reasonable. It was argued that "[t]he authority to search the person incident to a lawful custodial arrest, while based upon the need to disarm and to discover evidence, does not depend on what a court may later decide was the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect." (*ibid.*) Instead, the Court argued that a "custodial arrest of a suspect based on probable cause is a reasonable intrusion

[29] Riley v. California
[30] United States v. Robinson

under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification." (*ibid.*) In this decision, the Court chose not to differentiate the search of Robinson's person and the examining of the cigarette packet found. This is an important piece as it set the precedent to allow officers to search items found during the standard search incident to arrest, regardless of whether there is a concern for loss of evidence or the concern for the arrestee being armed.

Now that we've established the framework for the rationale behind the search incident to arrest principle, it must be applied to the case of Riley and his cell phone. It's clear that the cell phone is not a weapon. However due to its storage capacities, it can contain evidence. Yet, a cell phone cannot be compared to a crumpled package of cigarettes--its contents are not as easily found and identifiable as fourteen capsules of heroin. Chief Justice Roberts noted, "Cellphones...place vast quantities of personal information literally in the hands of individuals. A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in Robinson."[31] Additionally, digital data simply is not as harmful as weapons, drugs, or other physical evidence: the basis of which the search incident to arrest principle was established upon. Chief Justice Roberts even stated, "there are no comparable risks when the search is of digital data." (*ibid.*) However, Chief Justice Roberts went on to note that law enforcement officers reserve the right to, "examine the physical aspects of a phone to ensure that it will not be used as a weapon--say, to determine whether there is a razor blade hidden between the phone and its case." (*ibid.*) Chief Justice Roberts also made the point that today most phones automatically lock after a certain period of time. Thus, once the phone is locked, the

[31] Riley v. California

data becomes encrypted so searching would be near impossible. Consider the details of the San Bernadino case, in which a phone required a PIN for decryption because it had been powered down, encrypting all of the data inside it. Once a phone has become encrypted, the owner would need to provide the password or fingerprint to unlock the phone.[32]

Another important distinction to make is that cell-phones today are not comparable to cell-phones a mere few years ago. Chief Justice Roberts points out, "Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." (*ibid.*) Computers, and cell phones, are able to consolidate massive amounts of data in a small device. Chief Justice Roberts acknowledged, "Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy." (*ibid.*) However, advancement in technologies means that a search of a person can now intrude on incredible intimate details of their private lives. Because of this, the Fourth Amendment needs to consider computers, or any data storage device, as just that--a data storage device. Chief Justice Roberts quantified this data by noting, "the current top-selling smartphone has a standard capacity of sixteen gigabytes (and is

[32] Passwords can serve as the admittance of ownership, and thus fall under the protection of the Fifth Amendment. This thesis will not focus on the Fifth Amendment's role in computer searches.

available with up to sixty-four gigabytes). Sixteen gigabytes translates to millions of pages of text, thousands of photos, or hundreds of videos."[33]

So how do the storage capacities of computers relate to the Fourth Amendment? It deals most heavily with the association of privacy. As pointed out by Chief Justice Roberts, a cell phone today is a mini computer. This mini-computer is able to collect an immense amount of personal data and contain it all in one device. Chief Justice Roberts noted, "The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet." Additionally, the phone has the capability of containing data dating back to before the phone was even purchased. Chief Justice Roberts phrased it best when he explained "a person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone." (*ibid.*)

The data that is stored and found on cell phones is also much more explicit than what would traditionally be expected to be found during a physical search of a home. Chief Justice Roberts acknowledges that certain types of data are qualitatively different. For example, "an internet search and browsing history...can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns", and "historic location information is a standard feature on many smartphones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." (*ibid.*) This abundant amount of sheer personal data led the Court to state, "Allowing the police to scrutinize such records on a routine basis is quite different from

[33] Riley v. California

allowing them to search a personal item or two in the occasional case."[34] Finally, the issue with treating a cell phone as something as casual as a wallet or a crumpled up cigarette box is best summed up by Chief Justice Roberts when he stated, "Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form— unless the phone is." (*ibid.*)

The search incident to arrest principle was designed with good intentions. It was designed to protect people and ensure the justice system could not be corrupted by the destruction of evidence. It is still possible to maintain the integrity of this principle by extending it to the philosophy behind the Fourth Amendment. The United States Supreme Court acknowledged in Riley v. California that cell phones, or mini-computers, need to be handled differently under our current legal system. The same must be said for when computers are seized and searched under the Fourth Amendment. The restrictions and specifics of the warrant need to be different than that of traditional search warrants given the advanced technological nature of computers.

[34] Riley v. California

VI. Plain View Doctrine

One of the many hidden surprises of the Fourth Amendment is the Plain View Doctrine. There are exceptions to the warrant requirement for searches. If someone gives consent to a search, the search can take place. According to the use of the plain view doctrine in Coolidge v. New Hampshire, "if an officer is lawfully present, he may seize objects that are in 'plain view'. However, the officer must have had probable cause to believe that the objects are contraband."[35] For example, if a police officer has a search warrant for the presence of a dead body, and while looking around the house finds a greenhouse full of illegally growing marijuana plants, this would fall under the plain view doctrine. However, how should this apply to the search of a computer? It is important to note that the plain view doctrine was not created as yet another means for the government to search private homes. Instead, this was created to acknowledge that *sometimes* contraband can simply just be happened upon. Given the fact that this is something that happens rarely and isn't something that is explicitly searched for, when dealing with computers I argue that in order to fall under the plain view doctrine, files must be on the home screen or another location that is obvious.

Additionally, if files and folders are being searched in accordance with the previously mentioned stipulations, including the use of a third party and file type filters, then the file name or the content of the file can trigger the discovery. As mentioned above, the file type is what should be searched for rather than merely relying on the file extension. However, when dealing with the plain view doctrine, we must only rely on what would

[35] Coolidge v. New Hampshire

naturally be seen when investigating and searching for something. If while searching a privately owned residence for evidence of tax evasion, it would be fair to search through any financial documents. However, if while searching through these documents it is discovered that embezzlement has also occurred, then that is fair game. Similarly, if the image files on computers are being searched for child pornography, and photos of illegal drugs appear, then this too would be fair game and fall under the plain view doctrine. File names are also important, and should also serve as triggers. For example, if the searcher finds a file labeled "Child_Porn.png" then it would be reasonable to assume that this could possibly contain illegal content. This occurs more often than one would think. Recently it was discovered that the bombers who were responsible for the March 22nd, 2016 attack in Brussels had a folder on his laptop titled "Target".[36] As the plain view doctrine functions with physical searches, any discovered content outside the scope of the warrant must be something that only a third party search would have discovered and deemed possibly illegal.

[36] Brooks-Pollock, 2016

VII. Future Applications

The future of technological advancement is limitless. With computers becoming more portable and containing higher storage capabilities, privacy is becoming harder and harder to maintain. Consider cloud storage: we are now able to store our personal digital data on servers that are physically not owned by us. At that point, how does the law claim ownership if someone does not physically own the data? Additionally, cloud storage can be international. People can store information on servers in different countries, thousands of miles away. How then, can our legal system maneuver that? In Riley v. California, Chief Justice Roberts discusses the future of technology and states,

> "Mobile application software on a cell phone, or "apps," offer a range of tools for managing detailed information about all aspects of a person's life. There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life. There are popular apps for buying or selling just about anything, and the records of such transactions may be accessible on the phone indefinitely. There are over a million apps available in each of the two major app stores; the phrase "there's an app for that" is now part of the popular lexicon. The average smartphone user has installed 33 apps, which together can form a revealing montage of the user's life."[37]

[37] Riley v. California

With information being shared freely and abundantly, the lines upon which the Fourth Amendment was originally based on are blurring. As Justice Alito stated in United States v. Jones, "in circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."[38]

[38] United States v. Jones

VIII. Conclusion

Technology is advancing at a rate at which the law has simply not been able to keep up with. Our lives and daily routines are completely integrated with the use of computers, including laptops, tablets, smartphones, and even smart watches. An average smartphone today has the capacity to hold all of one's emails, contacts, messages, and can even track one's physical location through the GPS. In a way, computers have the capacity to contain all of the aspects that compose our life in digital format. Because of this, it is of utmost urgency and importance that the courts begin addressing the impact technology has on laws that were created at a time where something like a smartphone was unimaginable. In particular, the Fourth Amendment needs to be restructured in order to accommodate searches of computers. The existing legal background has shown how searches and seizures have adapted to new technology and new spaces. These precedent setting cases have pushed the boundaries on what both parties can legally do.

Given the importance of computers today, the courts must begin examining and determining the role the constitution and Fourth Amendment plays in computer searches. In summary, there are several aspects of the search warrant that must hold in order to conduct a constitutional and fair search: (1) When dealing with searching computers, search warrants must be explicit in exactly what they are searching for with reference to content and file/data types; (2) The scope of the search warrant needs to be specified before the warrant is executed; (3) The search warrant should specify a time limit for how long a computer can remain in the court's possession; (4) All searches of computers and the analysis on the data must be conducted by a third-party in order to avoid bias; (5)

Because computers do not present an inherent physical danger, they cannot be searched under the search incident to arrest principle; and (6) As the plain view doctrine functions with physical searches, any discovered content outside the scope of the warrant must be something that only a third party search would have discovered and deemed possibly illegal. With these restrictions and stipulations put in place, the Fourth Amendment can adequately and fairly be applied to computer searches today.

Works Cited

10 Works of John Adams 247–248 (C. Adams ed. 1856)

Brooks-Pollock, Tom. "Brussels Attacks: More Evidence Emerges That Terror Cell Were Planning Atrocities in Britain." *The Independent*. Independent Digital News and Media, 12 Apr. 2016. Web. 10 May 2016.

Carroll v. United States. United States Supreme Court. 2 March 1925. *United States Supreme Court*. 2 March 1925. Web. 05 May 2016.

"computer, n." *OED Online*. Oxford University Press, March 2016. Web. 13 May 2016.

Coolidge v. New Hampshire, 21 June 1971. *United States Supreme Court*. 21 June 1971. Web. 05 April 2016

"History of Fourth Amendment." *Justia Law*. Web. 13 Apr. 2016. <http://law.justia.com/constitution/us/amendment-04/01-search-and-seizure.html>.

Kerr, Orin S. "Ex ante regulation of computer search and seizure." *Virginia Law Review* (2010): 1241-1293.

Kerr, Orin. "Vermont Supreme Court Concludes That Magistrates Have the Discretion to Add at Least Some Kinds of Ex Ante Search Restrictions to Computer Warrants." *The Volokh Conspiracy.* N.p., 14 Dec. 2012. Web. 13 Apr. 2016.

"Kyllo v. United States." *Oyez.* Chicago-Kent College of Law at Illinois Tech, n.d. May 13, 2016. https://www.oyez.org/cases/2000/99-8508

Leagle. "U.S. v. MUTSCHELKNAUS." LEAGLE. N.p. 2015. Web. 14 April 2016.

Mason, Caleb. "Jay-Z's 99 Problems, Verse 2: A Close Reading with Fourth Amendment Guidance for Cops and Perps." *. Louis ULJ* 56 (2011): 567.

"Riley v. California." *Oyez.* Chicago-Kent College of Law at Illinois Tech, n.d. May 13, 2016. https://www.oyez.org/cases/2013/13-132

Riley v. California. United States Supreme Court. 25 June 2014. *United States Supreme Court*. 25 June 2014. Web. 05 May 2016.

Rosberg, Joe. "The One Terabyte Disk: Is It Reliable? - TechRepublic." *TechRepublic*. 30 July 2008. Web. 22 Apr. 2016.

U.S. v. Comprehensive Drug Testing, INC., et al, U.S. Court of Appeals for the Ninth Circuit, 18 December 2008. *U.S. Court of Appeals for the Ninth Circuit*. 18 December 2008. Web. 05 April 2016.

U.S. Const., amend. IV.

"United States v. Jones." *Oyez*. Chicago-Kent College of Law at Illinois Tech, n.d. May 13, 2016. https://www.oyez.org/cases/2011/10-1259

United States v. Jones, 23 January 2012. *United States Supreme Court.* 23 January 2012. Web. 05 April 2016

United States v. Robinson, 11 December 1973. *United States Supreme Court*. 11 December 1973. Web. 05 April 2016