Digital Effects: The Fourth Amendment and Computer Searches Warrants

Ash Moore

Follow this and additional works at: https://digitalcommons.law.ou.edu/okjolt

Part of the Fourth Amendment Commons

Recommended Citation
Available at: https://digitalcommons.law.ou.edu/okjolt/vol10/iss1/6
DIGITAL EFFECTS: THE FOURTH AMENDMENT AND COMPUTER SEARCHES

WARRANTS

© 2014 Ash Moore

Introduction

The Fourth Amendment 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 except upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.¹

This paper uses the physical computer and the Fourth Amendment to explore the larger concept of privacy rights in an increasingly digitized world. Part I traces the origin of the Fourth Amendment. Part II follows the Amendment’s development through its almost 300-year history. Part III explores how the Fourth Amendment and computers currently relate to one another. Part IV puts this paper’s discussion in a modern context and finally, Part V explains why physical computers deserve more protection than they currently receive because they now contain more “intimate details of the home” than any other object ever imagined.

I. A Long, Long Time Ago: The Origin of the Fourth Amendment

The maxim “a man’s home is his castle” can be traced to the seventh century in England.² But for centuries, this idea centered around protection from private actors, not state

¹ U.S. CONST. amend. IV.
² David E. Steinberg, Restoring the Fourth Amendment: The Original Understanding Revisited, 33 HASTINGS CONST. L.Q. 47, 63 (2005).
officials. It was not until the late fifteenth century, that the concept began to embrace protection from government intrusion as well as intrusion by private actors. It was at this time in history that home searches and seizures in England increased in frequency and violence. As a result, the English common law welcomed the idea that some government intrusions into the home were unreasonable and therefore, the wronged citizen therefore deserved compensation. The transition in thought and focus peaked in the 1760s with three famous cases.

The “paradigm search and seizure case for Americans” and the most famous case in America in the eighteenth century, revolved around a man named John Wilkes in England. John Wilkes was a member of the House of Commons and a severe critic of King George III. The Crown believed he was involved in a published anonymous letter sent to an opposition paper. The letter called the British Tory administration “wretched” puppets and “tools of corruption and despotism.” The Secretary of State, Lord Halifax, procured a single general warrant while attempting to enforce the seditious libel laws against John Wilkes and others.

General warrants were issued ex parte, immunized the government officials who executed them from civil trespass, and allowed searches and seizures without any proof of individualized suspicion. The warrants did not even require the person or the items to be seized

---

3 Id.
4 Id.
5 Id.
6 Id.
7 Id.
9 Id.
10 Steinberg, supra note 2, at 63.
11 Id.
12 Trepel, supra note 8, at 122.
13 Id. at 123.
be described. Because of their nature, warrants were often used to suppress political dissent in England and the American colonies by authorizing, “searches and seizures of all ‘trunks, studies, cabinets, and other repositories of papers’ for evidence of seditious libel.”14 In Wilkes’ case, one general warrant was used to search at least five houses and arrest forty-nine people.15 After execution of the warrant, Wilkes and his supporters filed at least thirty different lawsuits for trespass and false imprisonment.16 In the end, the warrant was declared null and void, the government officials were held liable for trespass, and a civil jury awarded Wilkes 4000 pounds in punitive damages.17 In addition to the punitive damage judgment, it is estimated that the British government spent more than 100,000 pounds defending the lawsuits.18

In one of the court opinions, Lord Camden stated, “the great end for which men entered society, was to secure their property.”19 Further, “that right is preserved sacred and incommunicable in all instances.”20 The only time property rights could be abridged were by laws passed for the public good.21 These laws only included those for “distresses, executions, forfeitures, and taxes.”22 Camden reiterated that in English common law, “‘every invasion of private property, be it ever so minute,’ was considered a trespass.”23 He believed this premise “is proved by every declaration in trespass where the defendant is called upon to answer for bruising

14 Id.
15 Steinberg, supra note 2, at 63.
16 Id.
17 Id.
18 Id.
20 Id.
22 Id.
23 Id.
grass and even treading upon the soil.”24 The burden was on the trespasser to justify or excuse his action.25 Camden believed that allowing the government’s actions “would be subversive of all the comforts of society.”26 But he also took time to distinguish the government’s right to enter the home to seize stolen goods and a few other instances by further referencing property rights.27 Camden was able to distinguish those situations.28 He did so by differentiating the government’s property rights in the items to be seized.29 However, when the object of the warrant was a private paper, as in the instant case, the government had no property interest in the papers and therefore no right to search for them or seize them.30

As a final note, Camden referenced the right against self-incrimination and said, “the law obligeth no man to accuse himself... and it would seem that search for evidence is disallowed upon the same principle.”31 This is what became known as the Mere Evidence Rule. Searches for profits of crime were allowed because the government had a property interest in those objects.32 On the other hand, the government could not search for “mere evidence” of a crime because the government obtained no property interest in private effects simply because they were somehow related to criminal activity of the owner.33

24 Id. at 311.
25 Id.
26 Id.
27 Id.
28 Id.
29 Id.
30 Id.
31 Id.
32 Id.
33 Id.
At the same time John Wilkes and his supporters were driving change in England, Charles Paxton was involved in a similar controversy in the American Colonies.\textsuperscript{34} Paxton was a customs officer who went to renew a writ of assistance in the Superior Court of Boston in 1761.\textsuperscript{35} A writ of assistance was a specialized form of general warrant.\textsuperscript{36} It authorized British custom officers to enter establishments, including homes, without suspicion, to search for untaxed goods (most commonly, tea and sugar).\textsuperscript{37} Beyond this basic blanket of authority, the writs also allowed officials to commandeer peace officers and ordinary citizens to aid in searches under the writs.\textsuperscript{38} However, unlike general warrants, the writs did not immunize the government officials from liability if they failed to uncover evidence of a crime.\textsuperscript{39} In spite of this, American colonists often found themselves suffering abuses under the writs, and over time, general resentment toward the writs grew.\textsuperscript{40}

As a result of the growing resentment, when Paxton went to renew his writ, an association of merchants in Massachusetts opposed the renewal in court.\textsuperscript{41} A renowned Boston attorney named James Otis represented the merchants and argued that freedom from government intrusion in one’s own home was “among the most essential branches of English liberty.”\textsuperscript{42} He furthered his argument against the writs of assistance by stating those instruments allowed officials to “enter our houses when they please...break locks, bars, and every thing in their way -

\begin{footnotes}
\footnotetext{34}{Steinberg, \textit{supra} note 2, at 64.}
\footnotetext{35}{Id.}
\footnotetext{36}{Trepel, \textit{supra} note 8, at 122.}
\footnotetext{37}{Id.}
\footnotetext{38}{Id.}
\footnotetext{39}{Id.}
\footnotetext{40}{Id.}
\footnotetext{41}{Steinberg, \textit{supra} note 2, at 64.}
\footnotetext{42}{M. H. \textit{Smith}, \textit{The Wrists of Assistance} Case 334 (1978).}
\end{footnotes}
and whether they break through malice or revenge, no man, no court can inquire.”43 Around the same time Otis opposed Paxton in the courtroom, resentment towards the writs reached a breaking point as American colonists violently opposed the Stamp Act in 1761 with a series of riots in the streets.44

It was just a little over a decade later when the First Continental Congress met.45 When the discussion turned to oppressive British action, the focus was mostly on official searches of homes.46 A couple years before, Samuel Adams, vehemently criticized writs of assistance for allowing such oppressive searches.47 He said, “Our homes and even our bedchambers are exposed to be ransacked, our boxes and chests and trunks broke open and plundered by wretches.”48 It was this sentiment, this fear and outrage, that was repeated at the Continental Congress. And it was this sentiment that lead to the Fourth Amendment.49

II. Moving On Up: The Evolution of the Fourth Amendment

The first time the Supreme Court confronted the limits and protections of the Fourth Amendment, it gave the Amendment a liberal construction. This action was based on a fear that a strict construction would allow the government to elevate form over substance and find loopholes in procedure to commit unconstitutional practices.50 The issue before the Supreme Court, that allowed them to lay the foundation for Fourth Amendment jurisprudence, revolved

---

43 Id.
44 Trepel, supra note 8, at 122.
45 Steinberg, supra note 2, at 66.
46 Id.
47 Id.
48 Id.
49 Id.
50 Clancy, supra note 21, at 313.
around a failure to pay taxes on thirty-five cases of plate glass. In the case, the defendant was subjected to a court order to produce invoices that the government believed would help prove an element of the case against the defendant. The order was issued pursuant to a provision in a customs revenue act. The provision of the act did not allow for searches and seizures, but simply required defendants to produce incriminating papers. However, if a defendant failed or refused to produce the papers, the Court treated the fact the government was seeking to prove by the papers as admitted by the defendant.

The Court found violations of the Fourth and Fifth Amendments in compelling the production of private papers. While the Court admitted that no search or seizure was authorized under the Act or in the immediate case, the effect of compelled production was substantially the same as the evils the Fourth Amendment sought to combat. The Court pointed out that the only difference was the lack of “aggravating incidents of actual search and seizure” like forcible entry in to a home. The Court announced, “it is not the breaking of his doors, and the rummaging of his drawers that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property.”

Even though the Court called property rights and a man’s security in them sacred, the Court still upheld searches in other contexts based on a property theory. The government could

---

51 Boyd v. United States, 116 U.S. 616, 617 (1886).
52 Id. at 618.
53 Id. at 617.
54 Id. at 621.
55 Id. at 618.
56 Id. at 621.
57 Id.
58 Id. at 622.
59 Id. at 630.
60 Id. at 623.
enter homes to search for stolen goods, goods a person had failed to pay taxes on, and in other listed situations based on the concept of superior property rights to the goods themselves. The government or an individual who the government was acting on behalf of had a superior right to the items and it was this right that permitted intrusion. In the case of private papers however, the Court said they are the owner’s “dearest property” and not subject to any other property interest.

In writing the opinion, Justice Bradley believed he was affecting the “very essence of constitutional liberty and security.” He believed the principles announced applied to “all invasions on the part of the government...of the sanctity of a man’s house and the privacies of his life.” The broad constitutional principles illustrated in the case became the foundation of Fourth Amendment jurisprudence and even though much of the case has been overruled, the Supreme Court still often returns to it when seeking inspiration for modern Fourth and Fifth Amendment rulings.

In all the ways Boyd was broad and aspirational, Olmstead was limiting and practical. In that case, government officials placed a wiretap on phone lines while investigating suspected violations of the National Prohibition Act. The government uncovered a conspiracy of “amazing magnitude” and ultimately tried to introduce the contents of the intercepted telephone

---

61 Id.
62 Id.
63 Id. at 627.
64 Id. at 630.
65 Id.
66 Clancy, supra note 21, at 313.
68 Id. at 455.
conversations at trial. The introduction was challenged by the defense and the case ultimately reached the Supreme Court, who was left to decide if the Fourth Amendment protected intercepted phone conversations.

The Court announced that the Fourth Amendment only protected material things (i.e. persons, houses, papers, and effects). Effects included things like letters, but where as in the instant case, “evidence was secured by the use of the sense of hearing and that only” and there was no entry in to a home or office, no search or seizure occurred. While the Court acknowledged the Amendment deserved liberal construction and broad interpretation, it refused to “justify enlargement of the language employed beyond the possible practical meaning of houses, persons, papers, and effects.” Ultimately, the Court only narrowed the protections of the Fourth Amendment to material objects. Additionally, the Court’s final decision also only safeguarded those objects from physical intrusions.

However, despite the majority opinion and the ruling in the case, it is the dissent, written by Justice Brandeis, that has become a staple of Fourth Amendment jurisprudence and analysis. Justice Brandeis reminded the Court that they must never forget “it is a Constitution we are expounding,” as the revered Chief Justice John Marshall once warned. “[Constitutions] are not ephemeral enactments, designed to meet passing occasions. They are, to use the words of Chief Justice Marshall, “designed to approach immortality as nearly as human institutions can

---

69 Id. at 457.
70 Id. at 455.
71 Id. at 464.
72 Id.
73 Id. at 465.
74 Id.
75 Id. at 472.
Because of this, Brandeis said, it was imperative to consider not only what was, but what may be. He observed that changing times had yielded new and farther-reaching means of invading privacy and he predicted that some day technology may give the government tools to reproduce sensitive documents in court without having to remove them from private drawers or even enter the homes of private citizens. These beliefs about the nature of Constitutions and predictions for the future caused Brandeis to chastise the Court and warn against too literal a construction. He warned that, “rights declared in words might be lost in reality.”

It was not until almost forty years after the majority’s narrowing of the Fourth Amendment and Brandeis’ warning in *Olmstead*, that the Supreme Court handed down what has become the leading case in Fourth Amendment jurisprudence. That case presented a second challenge to a wiretap by law enforcement officers, this time on the outside of a public phone booth. There, the Court refused to transform the Fourth Amendment into a general constitutional ‘right to privacy,’ but it nonetheless transformed Fourth Amendment jurisprudence. The majority proclaimed that, “the Fourth Amendment protects people, not places [and] what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.” On the other hand, “what [a man] seeks to preserve

---

76 Id.
77 Id. at 473.
78 Id. at 474.
79 Id.
80 Id. at 473.
83 Id. at 350.
84 Id. at 351.
as private, even in an area accessible to the public, may be constitutionally protected."\(^8^5\) The Court expressly rejected a Fourth Amendment analysis that would depend on the presence or absence of a physical intrusion into anything construed as a “constitutionally protected area,” whatever that may be.\(^8^6\)

This opinion transformed Fourth Amendment jurisprudence by rejecting what scholars call the property-based theories.\(^8^7\) Another case was decided within months of *Katz*, which rejected another aspect of the property-based theories, leading to what scholars believed to be their total demise.\(^8^8\) The Court came to believe that the emphasis of Fourth Amendment protection needed to shift its emphasis from property to privacy rights due to advancements in technology and “a subtle interplay of substantive and procedural reform.”\(^8^9\) Because of this, the *Katz* court believed Fourth Amendment protections were no longer limited to tangible property and property interests did not control whether a search or seizure had occurred.\(^9^0\) But as with *Olmstead*, it is not the majority opinion in *Katz* that has endured. Subsequent to the ruling in *Katz*, Fourth Amendment analyses began to take place under a two part “reasonableness” test, announced by Justice Harlan in his concurring opinion:\(^9^1\) First, a person must exhibit an actual (subjective) expectation of privacy; second, that expectation must be one that society recognizes as “reasonable” (objective).\(^9^2\)

\(^{8^5}\) *Id.*

\(^{8^6}\) *Id.* at 353.

\(^{8^7}\) Clancy, *supra* note 21, at 320.

\(^{8^8}\) *Id.*


\(^{9^0}\) Clancy, *supra* note 21, at 328.

\(^{9^1}\) *Id.*

\(^{9^2}\) *Id.*
It was this reasonableness test that governed Fourth Amendment protection when a defendant challenged law enforcement’s use of a thermal imager aimed at his home.\textsuperscript{93} Law enforcement officers believed the defendant was growing marijuana in his home in large quantities.\textsuperscript{94} Since this process would require a significant amount of high-intensity grow lights, the officers stood on a public street and pointed a thermal imager at the defendant’s home to determine if there was an abnormal amount of heat emanating from it.\textsuperscript{95} The defendant challenged action as an illegal search under the Fourth Amendment.\textsuperscript{96}

The Court began its analysis by repeating a previously announced determination that, “at its core,” the Fourth Amendment protects “the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.”\textsuperscript{97} On one hand, the Court cited Boyd and reiterated that, “the eye cannot by the laws of England be guilty of a trespass.”\textsuperscript{98} It was this rationale that always prevented the Court from requiring law enforcement officers to “shield their eyes when passing the home on public thoroughfares.”\textsuperscript{99} On the other hand, the Court pointed out that this was more than naked-eye surveillance and the issue was therefore how much technological enhancement of ordinary perception is too much from certain vantage points.\textsuperscript{100}

\textsuperscript{93} Kyllo v. United States, 533 U.S. 27 (2001).
\textsuperscript{94} \textit{Id.} at 29.
\textsuperscript{95} \textit{Id.}
\textsuperscript{96} \textit{Id.} at 30.
\textsuperscript{97} \textit{Id.} at 31 (citing Silverman v. United States, 365 U.S. 505, 511 (1961)).
\textsuperscript{98} \textit{Id.} at 32.
\textsuperscript{99} \textit{Id.}
\textsuperscript{100} \textit{Id.} at 33.
The Court concluded that the advancement of technologies had affected reasonable expectations of privacy in the home and elsewhere.\textsuperscript{101} It pointed out that previous decisions had shown advancements in aviation had exposed areas of the home to the public in lawful airspace when those areas were previously private.\textsuperscript{102} But the Court also felt there must be a limit to the “power of technology to shrink the realm of guaranteed privacy.”\textsuperscript{103} Ultimately the Court ruled “obtaining by sense-enhancing technology information regarding the interior of the home that could not otherwise have been obtained without physical ‘intrusion in to a constitutionally protected area’ constitutes a search - at least where (as here) the technology is not in the general public use.”\textsuperscript{104} The Court noted that the quality or quantity of the information gathered was completely irrelevant to the analysis because “physical invasion of the structure of the home, ‘by even a fraction of an inch,’ was too much” and there is no warrant exception for “the officer who barely cracks open the front door and sees nothing but the non-intimate rug on the vestibule floor.”\textsuperscript{105} In fact, the Court said case law makes it clear that all details of the home are intimate details, because the entire area is supposed to be shielded from the government.\textsuperscript{106}

Finally, recently the Supreme Court clarified that the property-based theory is not as dead as the critics claim. In the case at issue, law enforcement officials attached a GPS tracking device to the undercarriage of the defendant’s car and introduced the location data collected at his subsequent trial for conspiracy to distribute drugs.\textsuperscript{107} The Supreme Court found a Fourth Amendment violation due to the fact that the GPS device illegally (it was a trespass) occupied a

\begin{flushleft}
\textsuperscript{101} Id. \\
\textsuperscript{102} Id. at 34. \\
\textsuperscript{103} Id. \\
\textsuperscript{104} Id. at 34. \\
\textsuperscript{105} Id. at 37. \\
\textsuperscript{106} Id. \\
\end{flushleft}
private effect (i.e. the car) belonging to the defendant.\(^{108}\) The Court pointed out that this would have been a “search” within the meaning of the Fourth Amendment when it was adopted.\(^{109}\)

The Court traced the development of Fourth Amendment jurisprudence and noted the Amendment’s text revealed a close connection to property; It was this understanding of the language that led the Court to tie protections to common-law trespass concepts until the latter half of the twentieth century.\(^{110}\) The Court confronted the “reasonable expectation of privacy” test announced in and followed after \textit{Katz} but ruled that the instant case was not controlled by it.\(^{111}\) Instead, the Court clarified that the \textit{Katz}’s ruling simply established that property rights are not the sole measure for Fourth Amendment violations.\(^{112}\) In addition, the \textit{Katz} expectation of privacy test could never be used to diminish the protections the Fourth Amendment guaranteed when it was adopted and for this reason, the \textit{Katz} test simply adds to, but is not substituted for, a common-law trespassory test.\(^{113}\) The expectations of privacy protected under \textit{Katz} are ones that have their source outside of the Fourth Amendment “either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.”\(^{114}\)

As technology has advanced to allow searches that would have required physical intrusion at the time the Fourth Amendment was adopted, the Supreme Court has struggled to fashion tests, rules, and exceptions to them that protect individuals from governmental oppression. Physical trespass has always been the easiest way to determine if a search has occurred. But even though jurisprudence has necessarily expanded Fourth Amendment

\(^{108}\) \textit{Id.} at 949.

\(^{109}\) \textit{Id.}

\(^{110}\) \textit{Id.}

\(^{111}\) \textit{Id.} at 950.

\(^{112}\) \textit{Id.} at 951.

\(^{113}\) \textit{Id.} at 952. *

\(^{114}\) \textit{Id.} at 951.
protections as the nature of sensitive information and access to intimate details have begun to take on forms not contemplated by the Framers, the original protections have not changed. Physical intrusion is still a touchstone of Fourth Amendment analysis and the *Katz* test is utilized only when it is necessary to find a Fourth Amendment violation to uphold the intent of the Amendment in the absence of such an intrusion.

**III. The Computer and the Fourth Amendment**

Courts have failed at universally conceptualizing computers for the purpose of Fourth Amendment analysis. The most common conception is to view a computer as a container that holds numerous subcontainers of information (i.e. a filing cabinet). This view causes the computer to be treated more like a “place” than a “thing” (i.e. effect) for the purposes of Fourth Amendment analysis. Each folder or file is a distinct effect and therefore each folder or file requires its own Fourth Amendment justification before it can be legally searched. When individual files or folders are considered separate “things” to be searched, as in this sub-container perspective, Courts have struggled with determining the limits of searches authorized by computer warrants. In the past, lines have been drawn between encrypted and non-encrypted files as well as between password-protected user accounts.

Another court-accepted treatment of the computer treats the object like other containers under Fourth Amendment law. However, this view rejects the idea that the computer contains

---

115 Trepel, *supra* note 8, at 120.  
117 *Id.* at 119.  
118 *Id.* at 119-20.  
119 *Id.* at 119.  
120 *Id.*  
121 *Id.* at 113.
separate “subcontainers” and instead views the whole computer hard drive as one effect. This view removes any limitations and restrictions necessitated by the aforementioned subcontainer perspective. As long as the computer is lawfully seized, any file may be viewed.

The main problem with both these perspectives is the unique nature of computer hard drives. While computers are frequently analogized to filing cabinets to justify the container and subcontainer perspectives, some judges have refused to accept this analogy because computers are capable of storing much more information, a variety of ways, than any traditional filing cabinet was or is capable of doing. Due to this observation, some judges insist that computers must be treated differently than any other container under the Fourth Amendment. On the other hand, the Supreme Court once distinguished containers based on type but quickly abandoned such an approach because it was impractical and there was no basis for any distinctions in the language of the Fourth Amendment.

However, unique concerns presented by the nature of computers have led some courts to create a “special approach” for searching computers in spite of a lack of precedent. One thing courts try is to impose ex ante restrictions. An ex ante search requires a judge to pre-approve specific steps that limit the search. This could include limiting a search by a file names or

---

122 Id.
123 Id.
125 Id. at 203.
126 Id. at 216.
127 Id. at 216-17.
128 Id. at 202.
130 Id.
types on a computer.\textsuperscript{131} For physical searches, judges leave the details and methods of a search up to the discretion of the officers who execute the warrant.\textsuperscript{132} The only review that occurs is ex post, not ex ante, and it is a broad judicial review to ensure only that the methods were reasonable.\textsuperscript{133} The Supreme Court has explicitly rejected this approach for physical searches.\textsuperscript{134}

Two circuit courts have addressed ex ante restrictions on search warrants.\textsuperscript{135} In both cases, the courts had to address the problem of intermingled documents.\textsuperscript{136} In one case, the government seized several boxes of documents and took them off site to search them later.\textsuperscript{137} The boxes included documents that were evidence of criminal activity, but they also contained hundreds of other innocuous documents of a personal nature.\textsuperscript{138} When the seizure was challenged, the government argued that it would have been nearly impossible to search through all the documents on the site.\textsuperscript{139} While the court upheld the constitutionality of the search, it “suggested” that in future cases, law enforcement should seek prior judicial approval for the “wholesale removal” of such a large quantity of documents.\textsuperscript{140} The hope is that the over-broad seizure is monitored by a neutral and detached magistrate and is approved only in cases where it is justified by particular concerns.\textsuperscript{141}

\begin{flushright}
\textsuperscript{131} Clancy, \textit{supra} note 124, at 206.
\textsuperscript{132} Kerr, \textit{Searches and Seizures, supra} note 129, at 571.
\textsuperscript{133} \textit{Id.}
\textsuperscript{134} \textit{Id.}
\textsuperscript{136} \textit{Id.}
\textsuperscript{137} United States v. Tamura, 694 F.2d 591, 595 (9th Cir. 1982).
\textsuperscript{138} \textit{Id.}
\textsuperscript{139} \textit{Id.} at 595-96.
\textsuperscript{140} \textit{Id.}
\textsuperscript{141} \textit{Id.}
\end{flushright}
Twelve years after the above case was decided, scholars began to urge courts to apply the “Tamura rule” to computer searches.\textsuperscript{142} It is not possible to physically separate information stored in a computer so searches of a computer will inevitably involve intermingled documents.\textsuperscript{143} However, while the Tamura case only asks that law enforcement officials request prior approval for the wholesale removal of numerous intermingled documents, the “Tamura rule” scholars asked the courts to apply to computer warrants included a new requirement that the warrants relate specific search protocols to explain how the officer will sort through the documents on a computer and gather evidence.\textsuperscript{144} The reasoning behind this addition was that the Tamura rule was premised on exigent circumstances to prevent the destruction of evidence.\textsuperscript{145} However, once computers are taken by law enforcement, the exigency passes and law enforcement officers should not be allowed to look through computers any way they want and at their own pace.\textsuperscript{146} Even though this method truly originated in a law review article and not in a previous court case, one court relied on it when it handed down an ultimately influential case.\textsuperscript{147}

In that case, an officer searched a computer pursuant to a search warrant that authorized him to look for evidence relating to a drug offense.\textsuperscript{148} While he was searching however, the officer found child pornography.\textsuperscript{149} The officer abandoned the search for drug evidence and

\begin{itemize}
\item \textsuperscript{142} Kerr, \textit{Searches and Seizures}, \textit{supra} note 129, at 572.
\item \textsuperscript{143} Winick, \textit{supra} note 135, at 105.
\item \textsuperscript{144} Kerr, \textit{Searches and Seizures}, \textit{supra} note 129, at 572.
\item \textsuperscript{145} Winick, \textit{supra} note 135, at 106.
\item \textsuperscript{146} \textit{Id.}
\item \textsuperscript{147} \textit{Id.} at 573.
\item \textsuperscript{148} Carey & United States v. Gary, 172 F.3d 1268, 1270-71 (10th Cir. 1999).
\item \textsuperscript{149} \textit{Id.} at 1276.
\end{itemize}
began searching for more images of child pornography. The government argued that the additional images found fell under the plain view exception to the warrant requirement. Ultimately, the court decided that the search for additional images was improper and beyond the scope of the warrant. The court said, “where officers come across relevant documents so intermingled with irrelevant documents (i.e. computer hard drives) that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents.” The court further said that reliance on analogies to other closed containers may lead courts to “oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage.” In a case following the one above, the same circuit made it clear that the “special approach” it condoned was one that may require “an intermediate step of sorting various types of documents.”

Despite this method’s popularity, commentators have almost uniformly criticized it. The first is the fact that it requires ex ante restrictions when courts have explicitly rejected this approach in other contexts. The second concern is about the general nature of computer searches that the method tries to avoid. When the Tamura rule was first applied to computers, the average home computer could only store the equivalent of around 100,000 typewritten

---

150 Id.
151 Id. at 1272.
152 Id. at 1276.
153 Id. at 1275.
154 Id.
155 United States v. Campos, 221 F.3d 1143, 1146 (10th Cir. 2000).
156 Trepel, supra note 8, at 124.
157 Kerr, Searches and Seizures, supra note 129, at 572.
158 Trepel, supra note 8, at 125.
pages.\textsuperscript{159} Today however, common computers can store the equivalent of over forty million typewritten pages.\textsuperscript{160} That is over 800 times the storage capacity in less than thirty years. Finally, the last criticism is that the Tamura method assumes file names accurately reflect the contents.\textsuperscript{161}

Due to these concerns, other courts have developed their own “special approach” methods. Some courts interpret the particularity requirement for warrants to require the specific evidence sought and not merely the computer hardware.\textsuperscript{162} Other courts require warrants to state the purpose the computer is being seized for.\textsuperscript{163} At least one court treats folder labels (but not their contents) as being in plain view.\textsuperscript{164} Finally, some courts require officers to use advanced search tools when those tools are sufficient to capture the sought after evidence.\textsuperscript{165} This list does not represent an exhaustive illustration of all the methods employed by courts, however, as the methods courts use are almost as numerous as the courts themselves.\textsuperscript{166}

These struggles, coupled with other advancements in technology, later interpretations of the \textit{Katz} case, and the original intent of the Fourth Amendment, have led scholars to believe the Fourth Amendment is incapable of protecting privacy interests in the modern society.\textsuperscript{167} As a result, additional privacy protections have been developed, mostly by Congress, to fill the gap between the Fourth Amendment protections and what reasonable people want and expect.\textsuperscript{168} The beginning of this understanding came with wiretapping technology. As the history of the Fourth Amendment

\begin{itemize}
\item[\textsuperscript{159}] Winick, \textit{supra} note 135, at 81.
\item[\textsuperscript{160}] Trepel, \textit{supra} note 8, at 125.
\item[\textsuperscript{161}] \textit{Id}.
\item[\textsuperscript{162}] \textit{Id.} at 124.
\item[\textsuperscript{163}] \textit{Id}.
\item[\textsuperscript{164}] \textit{Id}.
\item[\textsuperscript{165}] \textit{Id}.
\item[\textsuperscript{166}] \textit{Id}.
\item[\textsuperscript{167}] Kerr, \textit{Fourth Amendment, supra} note 81, at 838.
\item[\textsuperscript{168}] \textit{Id}.
\end{itemize}
Amendment (discussed above) relates, wiretapping technology made the Supreme Court change its understanding of the law and technology and how the two intertwine. While the Court originally failed to recognize that the Fourth Amendment should regulate wiretapping technology, it eventually understood the importance of the technology. As a result, it ultimately constitutionalized and effectively regulated the practice with subsequent cases.

When cases made it clear wiretapping was constitutional within certain bounds, Congress immediately took over and passed several statutes. These included the Federal Wire Interception Act, the Electronic Surveillance Control Act, and the Federal Wiretap Act. The latter of which (also known as Title III) is still the governing law today. The acts themselves were challenged in court but because they incorporated the teachings of the Supreme Court cases decided around the same time, they survived constitutional scrutiny. Today, the act of wiretapping is controlled by a federal statutory scheme, and not the Fourth Amendment or the courts. So, if a wiretap is challenged today, it is challenged on statutory grounds.

Wiretapping is not the exception when it comes to new technologies and privacy protections. In most cases of new technology and individual rights, congress has acted quickly and decisively leaving only a secondary role for the courts and the Fourth Amendment. At times, Congress has acted in response to Supreme Court decisions. For instance, when the

---

169 Id. at 839.
170 Id.
171 Id. at 850.
172 Id.
173 Id.
174 Id.
175 Id.
176 Id. at 855.
177 Id.
178 Id.
Supreme Court ruled that the Fourth Amendment did not protect pen register information (numbers dialed from telephones), Congress passed a law doing just that.\textsuperscript{179} At other times, Congress has acted on its own without any spurring from the courts. Without any legal challenge, Congress passed the Privacy Act of 1974 that allows citizens to check and correct information about themselves in government databases.\textsuperscript{180} With this practice as a reference, it is all the more notable that the courts have been left to struggle with the problems with computer search warrants.

\textbf{IV. Back to the Future: Modern Context for Fourth Amendment Analysis}

As early as 1890, Judges and Justices began struggling with technology and privacy rights.\textsuperscript{181} When considering the Kodak camera and the tabloid press, Justice Brandeis and Samuel Warren opined, “Gossip is no longer the resource of the idle and of the vicious but has become a trade.”\textsuperscript{182} In addition, it was over forty years ago that the United States Department of Health, Education, and Welfare (renamed the Department of Health and Human Services in 1979) investigated looming threats to individual privacy.\textsuperscript{183} The agency concluded that one of the most dangerous threats was accumulated personal information located in computerized federal databases.\textsuperscript{184} However, it was not until twenty years later that instantaneous information storage and transfer on a massive scale became possible and profitable due to computer

\textsuperscript{179} Id.
\textsuperscript{180} Id.
\textsuperscript{182} Id.
\textsuperscript{184} Id.
technology.\textsuperscript{185} Once technology was advanced enough to make the collection of personal information profitable, private companies began storing and transferring massive amounts of data in the same manner in which government agencies had previously employed.\textsuperscript{186} This gave rise to the term “Little Brother” playing off of George Orwell’s famous depiction of an omniscient and oppressive government embodied in “Big Brother.”\textsuperscript{187} Therefore, the information industry had a huge effect on turning sacrosanct pieces of private information into little more than a Wall Street commodity.\textsuperscript{188} And when the Internet came along, the process of data collecting was streamlined to the point where private companies and government agencies could exponentially increase the volume of information contained in vast and numerous databases.\textsuperscript{189}

The Internet, at the most basic level, is the largest computer in the world.\textsuperscript{190} Almost fifteen years ago a computer technology company Chief Executive Officer famously said, “You have zero privacy [on the internet]. Get over it.”\textsuperscript{191} But the Internet deserves credit for more than just possibly causing the “death of privacy.”\textsuperscript{192} It is also responsible for the digitization of expression that has been called “the end of forgetting.”\textsuperscript{193} It is estimated that the average social media user creates seventy pieces of content each month.\textsuperscript{194} Once created, this content exists infinitely in cyberspace and even if it is “deleted” technologically savvy people can almost

\textsuperscript{187} Id.
\textsuperscript{188} Bunker et al., \textit{supra} note 185, at 582.
\textsuperscript{189} Id.
\textsuperscript{191} A. Michael Froomkin, \textit{The Death of Privacy?}, 52 Stan. L. Rev. 1461, 1462 (2000).
\textsuperscript{192} Id.
\textsuperscript{193} Rosen, \textit{supra} note 181.
\textsuperscript{194} Id.
always still find it somewhere in the dark corners of the web.\textsuperscript{195} In a 2010 study conducted by Microsoft, seventy-five percent of employers required online research in to applicants that covered social media, online gaming, blog, and photo and video sharing sites.\textsuperscript{196} But the Internet, like physical computers, stores more than consciously created information.\textsuperscript{197} Other Internet (especially social media) users can create content about a person he or she has no knowledge about or control over.\textsuperscript{198} In addition, web sites track and store the metadata similar to physical computers.\textsuperscript{199} At the very least, this data includes information about how many times and how long a specific user visits a site..\textsuperscript{200}

In mid-2013, Edward Snowden became the biggest whistleblower in the National Security Agency’s history when he leaked over a million and a half documents.\textsuperscript{201} The first set of documents revealed the extent of the Agency’s surveillance of mobile phones in the United States.\textsuperscript{202} Another set of documents detailed a program called XKeyscore that allows analysts to search e-mails, browsing histories, and social media activity (information commonly called metadata) of millions of individuals with no prior authorization.\textsuperscript{203} In short, this program helps federal agents collect, monitor, and use against any person anything that person does on the

\textsuperscript{195} Id.
\textsuperscript{196} Id.
\textsuperscript{197} Id.
\textsuperscript{198} Id.
\textsuperscript{199} Id.
\textsuperscript{200} Id.
Internet. Snowden said that the program would let him wiretap anyone from anywhere with no more than a personal e-mail address.

Snowden’s leaks ultimately revealed an international effort to create a global surveillance network. The United States, Britain, Australia, Brazil, Canada, Denmark, France, Germany, Italy, Israel, the Netherlands, Norway, Spain, Sweden, and Switzerland have all been involved at one level or another. All these countries have been involved in monitoring or accessing computer user information. Snowden’s leaks showed that everything a person does on the Internet or their mobile phone is or can easily be monitored with no particularized warrant or suspicion for a specific person. Proving, once and for all, that there is in fact, no actual privacy on the Internet or on a mobile phone. Currently, there is a circuit split over the constitutionality of the NSA’s collection of phone records. While a Washington judge compared the program to something from Orwell’s 1984, a judge in New York upheld the program for national security reasons. This means no one knows the fate of this program, similar programs, or privacy rights of the world’s citizens at this point in time.

V. Analysis

In modern society, information is one of the most valuable commodities a person possesses. The value of information can be seen every day when identities are stolen for fraud. People use other peoples’ information to get credit cards or to invest or steal assets. The

\[\text{Id.}\]
\[\text{Id.}\]
\[\text{Id.}\]
\[\text{Id.}\]
\[\text{Id.}\]
\[\text{Id.}\]
\[\text{Id.}\]
\[\text{Id.}\]
information is highly sought after, not only by criminals and others who seek it for sinister purposes, but also by companies in the ways and for the purposes listed above. Companies use the information to target consumers more effectively and directly. But as the Snowden leaks reveal, the government also seeks personal information on a massive scale. The government uses and stores this information to track individuals in and out of the United States. While the information on most individuals will sit in massive databases never to see the light of day, some people will see the information used against them in court or at the very least in criminal investigations. While the constitutionality of the program is in question, what is not in question is the national outrage and debate it has sparked. Many people did not know the government kept such massive records and now the debate is over whether the government should even be allowed to compile so much personal data from private citizens.

With the ever-increasing capabilities of smartphones, such devices are becoming more like computers at an exponential rate. Computers are becoming exponentially more powerful and more integrated in to the every day life of Americans. It is more common to communicate by e-mail than it is physical or “snail mail.” Online shopping is continuously growing in popularity. People are increasingly connected through online gaming and other instantaneous forms of communication and connectivity. Now instead of driving to an office or flying to another city, companies can conduct meetings through the Internet or phone lines. Because technology, especially the computer and the Internet, is becoming so integrated in to every day life, it has become nearly if not completely impossible to shut oneself off from it if someone wants to continue to be able to function in modern society. The nature of society is that people are forced to use computers and the Internet, all the while, having little to no protection for their private information. Just because this is the way things are, does not mean that it is the way they should
be. However, as of now, it seems not even the circuit courts can agree on how much personal information and privacy should be protected.

When dealing with the computer and the privacy rights implicated by a search of it, the courts have struggled to come up with a sufficient analogy. Early analogies compared the computer to filing cabinets. This is because the terminology is similar and the concept is easy to understand. A computer holds individual files. Those files are separate and distinct from one another even though they are all in one location. The problem is that the types of files a computer holds can be very different from the types of files someone puts in a file cabinet. Furthermore, computers now hold much more information than any filing cabinet can. Moreover, “metadata” poses a unique risk that a filing cabinet does not. A filing cabinet does not store how many times a file has been accessed, who accessed it, and what the person used the information for. A filing cabinet does not tell someone the last time it was opened or how long it was open. It does not tell someone where the people who used it came from or where they went. It does not connect to other filing cabinets and transfer sensitive information, such as credit card and social security numbers, while leaving a trail and a copy of the information transmitted. So the question is whether there is an appropriate analogy to the physical world that the court can employ.

When considering the amount and types of information a computer stores, how many different things a computer is used for in modern society, and how integrated into a person’s life a computer inevitably is, any analogy to a personal paper or effect seems to fall very short of the mark. It seems that a computer deserves more protection than any other possession in the world. Considering this, there are two other things listed in the Fourth Amendment that courts have historically, fiercely protected. There is a person’s physical body and a person’s home. No matter how integrated computers are in our lives, they are not part of our physical bodies (not yet at
least). On the other hand, as technology advances and the Internet becomes more indispensable, there is more discussion about “online presence.” There is a digital version of every person who ventures online. Should that digital body of information and data be treated like the physical body of a person? Should courts begin to look at information that comprises an online presence and analyze it along the same lines that they analyze physical intrusions? Is there a way to create a dividing line in the digital world that makes sense the way dividing lines in the physical world do? Or would they be more arbitrary and ineffective?

In addition to physical bodies however, the Fourth Amendment has always protected the home with fervor as well. Courts have repeatedly cited the “intimate details of the home” as the reason for this protection. Courts have discussed the fact that the home is where most of the decisions for the family are made. It is where most intimate moments occur. It is where people not only feel they are, but also that they should be, protected the most from intrusion. But computers and technology are changing the way families communicate. Instead of waiting until after school to get a note from a teacher when a child has acted up, parents can be e-mailed or texted immediately. Parents no longer have to be in the same room to make important family decisions. Bills are not viewed or paid in paper form anymore. Most are viewed and paid online, with every member of the family aware of the password, capable of accessing the information. Internet connected remotes and smartphone applications enable people with high electric bills to change the settings from across the street or across the Atlantic for that matter. A person’s and a family’s whole life can be accessed through their computer. All the intimate details of the home that the Framers were concerned with protecting can now be accessed on a family’s computer. Is the move to a more digital life one of the advancements in technology that caused the focus of Fourth Amendment jurisprudence to shift from property interests to privacy expectations in the
first place? Does this advancement in technology warrant another shift in Fourth Amendment jurisprudence?

It is obvious that the filing cabinet analogy is obsolete. Is an analogy to the home or body more appropriate? Should a personal computer be compared to a home? If so, does that make its Internet connections more like streets? Just because a street brings you directly to the home does not mean it gives you the right to access the personal and intimate details the home possesses. Just like the Court forbid police officers from using advanced technology in *Katz* to view “intimate details of the home” from a public thoroughfare, should a court refuse to let law enforcement use computer programs from the internet to collect and access the same kind of information stored on a personal computer? Does the form of the information matter in this context or is it the substance that the Fourth Amendment should protect?

The Court has encountered this dilemma before with changing technologies. When wiretapping and technological surveillance became common, the Court decided it was the substance of the information that mattered under the law. It was a person’s reasonable expectation of privacy that determined whether the information was protected. However, in a world where computers and information stored on them are constantly monitored, can a person claim an actual expectation of privacy in digitally stored information anymore? Should a person be able to claim such an expectation? Would laws need to be rewritten or created to grant an expectation of privacy in a media where there currently is not one? Does it matter that people are being forced to join the digital revolution by the nature of society, whether or not they are comfortable with the effect of such a shift in ideology on their personal privacy?

The personal computer and devices with similar capabilities are inevitably intertwined in to every day life now. Whether a person wants privacy or not is irrelevant because almost
everyone needs to use digital resources to function in society. Is a Constitution that was written in a world without a digital element capable of being expounded so far as to protect digital rights? Are there digital rights?

**Conclusion**

As integrated as computers are and as much sensitive information as they store, they should not be treated like any other effect a person owns. They should be sacrosanct. They should receive the highest constitutional protections. The framers emphasis on protecting the home, property, and bodies of individuals was not simply to protect them from physical intrusion. As the courts have recognized before, it was the intimate details possessed and stored in these places that the Framers were really trying to protect. This is why current legal conceptions of computers and digital presence are insufficient. If Congress refuses to step in, the way it did with wiretapping technologies, the Court should recognize the sanctity of the Framers intent again.

As Edward Snowden showed the world when he leaked the NSA documents, the government has already trampled on and disregarded any privacy interests a person may have in their digital information. It is because of this that the Court may not be able to wait for Congress to act. In addition, as Chief Justice John Marshal once so eloquently put it, “it is emphatically the province and duty of the Court to determine what the law is.” If there is any modern hope of finding privacy in a digital life, the Court must act sooner rather than later. The physical computer and Fourth Amendment warrant requirements are simply one piece of a larger, more complicated puzzle. When the pieces are put together in the future, the picture can be one that emphasizes individual rights and liberties, the way the Framers intended. On the other hand, the ultimate image could be one of government being able to constantly monitor and collect data.
about its citizens in a way the framers never could have imagined. The technologies may be new and the issues seemingly more complicated than before, but the struggle between government power and individual rights is as old as society itself. The Founding Fathers tried to answer this question for our society long ago. They struck a balance for us that we have claimed to respect. Now more than ever it is important to determine whether we want to honor only their carefully chosen words, or their overall message as well.