

---

## LET'S BE REASONABLE: FOURTH AMENDMENT PRINCIPLES IN THE DIGITAL AGE

SCOTT D. BLAKE\*

Cite as: Scott D. Blake, *Let's Be Reasonable: Fourth Amendment Principles in the Digital Age*, 5 SEVENTH CIRCUIT REV. 491 (2010), at <http://www.kentlaw.edu/7cr/v5-2/blake.pdf>.

### INTRODUCTION

A police officer comes to your house, knocks on your door, and presents you with a search warrant. The warrant authorizes the officer to search your house for any evidence of illegal drug activity. This includes any physical evidence, such as drugs, pipes, syringes, cash, or storage containers, as well as any computers that may store incriminating digital files.<sup>1</sup> During the search, the officer discovers a substantial amount of marijuana, baggies, a scale, and other drug paraphernalia.<sup>2</sup> The officer also seizes your laptop and takes it back to the police station so its contents can be examined.<sup>3</sup>

The following week, a police detective begins to search the laptop. First, he makes an exact copy of your hard drive to prevent any files from being destroyed.<sup>4</sup> Next, the detective uses a sophisticated software program that organizes every file on your laptop and creates a directory, which he proceeds to examine.<sup>5</sup> After opening dozens of

---

\* J.D. candidate, May 2011, Chicago-Kent College of Law, Illinois Institute of Technology.

<sup>1</sup> See *United States v. Burgess*, 576 F.3d 1078, 1083 (10th Cir. 2009).

<sup>2</sup> See *United States v. Carey*, 172 F.3d 1268, 1270 (10th Cir. 1999).

<sup>3</sup> See *id.*

<sup>4</sup> See *Burgess*, 576 F.3d at 1083–84.

<sup>5</sup> See *United States v. Mann*, 592 F.3d 779, 781 (7th Cir. 2010).

innocent files, the officer opens a folder that contains hundreds of JPG image files.<sup>6</sup> He opens the first file that reveals a picture of a young boy, naked and posing for the camera.<sup>7</sup> The officer makes a notation, but moves forward with his original search for drug-related activity.<sup>8</sup> His subsequent search reveals more photos of child pornography, as well as other incriminating drug-related files. The police then arrest you and charge you for both the sale of marijuana and possession of child pornography.

This factual scenario is very similar to a number of cases playing out in the federal circuits involving the inadvertent discovery of illegal files that are outside the scope of the warrant during a computer search.<sup>9</sup> Defendants typically challenge the admissibility of this type of evidence in a motion to suppress arguing that the search and seizure was beyond the scope of the original warrant.<sup>10</sup> On the other hand, prosecutors and law enforcement argue that this type of evidence is admissible because it falls under the plain view doctrine.<sup>11</sup>

Courts have wrestled over whether inadvertently discovered computer files are properly admissible under the plain view doctrine, or whether they are inadmissible because the search and seizure was beyond the scope of the original warrant.<sup>12</sup> A majority of federal circuits, including the Seventh Circuit in *United States v. Mann*,<sup>13</sup> have extended traditional Fourth Amendment warrant doctrine to the realm of digital evidence.<sup>14</sup> These courts base their analyses on three

---

<sup>6</sup> See *United States v. Gray*, 78 F. Supp. 2d 524, 527 (E.D. Va. 1999).

<sup>7</sup> See *id.*

<sup>8</sup> See *Mann*, 592 F.3d at 781.

<sup>9</sup> See *United States v. Williams*, 592 F.3d 511, 514 (4th Cir. 2010); *Mann*, 592 F.3d at 782; *United States v. Carey*, 172 F.3d 1268, 1271 (10th Cir. 1999); *Gray*, 78 F. Supp. 2d at 528.

<sup>10</sup> See *id.*

<sup>11</sup> See *Williams*, 592 F.3d at 519; *Mann*, 592 F.3d at 782.

<sup>12</sup> See *Williams*, 592 F.3d at 514; *Mann*, 592 F.3d at 782; *Carey*, 172 F.3d at 1271; *Gray*, 78 F. Supp. 2d at 528.

<sup>13</sup> 592 F.3d at 786.

<sup>14</sup> See generally *Williams*, 592 F.3d 511; *United States v. Burgess*, 576 F.3d 1078 (10th Cir. 2009); *United States v. Miranda*, 325 F. App'x 858 (11th Cir. 2009); *United States v. Turner*, 169 F.3d 84 (1st Cir. 1999); *United States v. Henson*, 848 F.2d 1374 (6th Cir. 1988).

foundations of Fourth Amendment doctrine: reasonableness, the particularity requirement, and the plain view doctrine.<sup>15</sup>

In contrast, the Ninth and Tenth Circuits question whether traditional Fourth Amendment doctrine sufficiently protects privacy rights in the digital age.<sup>16</sup> In response, both Circuits have deviated from traditional Fourth Amendment principles.<sup>17</sup> The Ninth Circuit has advocated a multi-step prophylactic approach in order to prevent overbroad searches, and the Tenth Circuit determines whether the search has exceeded the scope of the warrant by looking at the subjective intent of the executing officer.<sup>18</sup>

Both of the Ninth and Tenth Circuits' deviations are premature and create just as many issues as they solve. They are premature because traditional Fourth Amendment doctrine has proved to be workable in digital evidence cases. Over time, the contours of Fourth Amendment doctrine will evolve along with developments in computer technology. The divergence is also impractical because it would act as a constitutional straitjacket on law enforcement working the field and would create two systems of search and seizure law—one for physical evidence and one for digital evidence. These two approaches are unnecessary because traditional Fourth Amendment doctrine provides sufficient constitutional protection to individuals and will evolve as technology develops or possible constitutional intrusions later arise.

#### I. FRAMING THE ISSUE: TRADITIONAL FOURTH AMENDMENT DOCTRINE

In order to fully understand the issue before the Seventh Circuit in *United States v. Mann*, it is important to understand

---

<sup>15</sup> *See id.*

<sup>16</sup> *See United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1006–07 (9th Cir. 2009); *Carey*, 172 F.3d at 1273–76.

<sup>17</sup> *See id.*

<sup>18</sup> *See id.*

traditional Fourth Amendment doctrine. The starting point for this analysis is the language of the Fourth Amendment itself, which states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.<sup>19</sup>

Since the text clearly indicates that individuals are protected from any “unreasonable searches and seizures,”<sup>20</sup> the Supreme Court has held that reasonableness is the touchstone of any Fourth Amendment analysis.<sup>21</sup> Drawing a clear line between a reasonable and unreasonable search is difficult; therefore, courts must examine and balance the totality of the circumstances.<sup>22</sup> A search’s reasonableness “is judged by balancing its intrusion on the individual’s Fourth Amendment interests against its promotion of legitimate governmental interests.”<sup>23</sup> For example, in *Polston v. State*, the Supreme Court of Arkansas upheld a state statute that subjected convicted felons to mandatory DNA testing.<sup>24</sup> The court held that the statute was reasonable because the felons’ privacy interests were outweighed by both the state’s interest in having an accurate criminal justice system and an interest in preventing and solving future crimes.<sup>25</sup>

---

<sup>19</sup> U.S. CONST. amend. IV.

<sup>20</sup> *Id.*

<sup>21</sup> *Illinois v. McArthur*, 531 U.S. 326, 330 (2001); *Katz v. United States*, 389 U.S. 347, 359 (1967).

<sup>22</sup> *United States v. Banks*, 540 U.S. 31, 36 (2003) (holding that the Court has “treated reasonableness as a function of the facts of cases so various that no template is likely to produce sounder results than examining the totality of circumstances in a given case”).

<sup>23</sup> *Delaware v. Prouse*, 440 U.S. 648, 654 (1979).

<sup>24</sup> 201 S.W.3d 406, 407–08 (Ark. 2005).

<sup>25</sup> *Id.* at 410–11 (“As to the felon’s expectation of privacy, the United States Supreme Court has recognized that ‘those who have suffered a lawful conviction’

### A. General Searches are Unreasonable

General searches are per se unreasonable.<sup>26</sup> The Fourth Amendment aims to protect individual privacy rights by preventing law enforcement from conducting general searches that result in a rummaging through an individual's property until something incriminating is found.<sup>27</sup> In order to prevent general searches, the Fourth Amendment requires the police to obtain a warrant from a judge before conducting a search.<sup>28</sup> A judge may issue a warrant only when there is probable cause to believe that what the police are looking for will be in the place to be searched.<sup>29</sup>

### B. The Particularity Requirement

A warrant may be issued once probable cause has been established.<sup>30</sup> However, the warrant must “particularly describe the things to be seized” so that “nothing is left to the discretion of the officer executing the warrant.”<sup>31</sup> This particularity requirement ensures that the search will be narrowly tailored and “will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.”<sup>32</sup> For example, the particularity requirement was not met when a magistrate issued a warrant only referencing a search for a “single dwelling [residence] . . . blue in color.”<sup>33</sup> Although the police had probable cause to look for illegal weapons and explosives,

---

are subject to a ‘broad range of [restrictions] that might infringe constitutional rights in a free society.’” (quoting *McKune v. Lile*, 536 U.S. 24, 36 (2002))).

<sup>26</sup> *Coolidge v. New Hampshire*, 403 U.S. 443, 454–55 (1971).

<sup>27</sup> *Id.* at 467 (holding that the Fourth Amendment protects against general warrants that would authorize an “exploratory rummaging in a person’s belongings”).

<sup>28</sup> *Maryland v. Dyson*, 527 U.S. 465, 466 (1999).

<sup>29</sup> *United States v. Ross*, 456 U.S. 798, 824 (1982).

<sup>30</sup> *Id.*

<sup>31</sup> *Marron v. United States*, 275 U.S. 192, 196 (1927); *see also* *Stanford v. Texas*, 379 U.S. 476, 485 (1965).

<sup>32</sup> *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

<sup>33</sup> *Groh v. Ramirez*, 540 U.S. 551, 558 (2004).

the language in the warrant “did not describe the items to be seized *at all*.”<sup>34</sup> By failing to particularly describe the “place to be searched” or “the persons or things to be seized,”<sup>35</sup> the warrant failed to meet the particularity requirement and was therefore unconstitutional.<sup>36</sup>

While executing a warrant, a police officer may only search and seize items specified in the warrant.<sup>37</sup> Again, a reasonableness standard is applied to determine whether the evidence seized was within the scope of the warrant.<sup>38</sup> For example, “[i]f you are looking for an adult elephant, searching for it in a chest of drawers is not reasonable.”<sup>39</sup> However, the hypothetical at the beginning of this Note provides a more realistic illustration. There, the officer was authorized to search anywhere in the house where illegal drugs could reasonably be located.<sup>40</sup> The officer could open and examine the freezer door, the desk drawer, a storage box, kitchen cabinets, and so on to attempt to find illegal drugs. But his search must remain within the bounds of reasonableness.<sup>41</sup> For example, it might be unreasonable to search the defendant’s tax records if the warrant did not authorize a search for financial documents in connection with drug trafficking.<sup>42</sup>

### *C. The Plain View Doctrine*

What if the officer opens a box in the basement while looking for drugs, but instead inadvertently discovers hundreds of photos of child pornography? The child pornography is clearly outside the scope of the search warrant. But since the criminality of the photos is so patently obvious, it would be illogical for the law to require the officer to ignore this incriminating evidence. In response, the Supreme Court

---

<sup>34</sup> *Id.* (emphasis in original).

<sup>35</sup> U.S. CONST. amend. IV.

<sup>36</sup> *Groh*, 540 U.S. at 558.

<sup>37</sup> *Walter v. United States*, 447 U.S. 649, 656 (1980).

<sup>38</sup> *Florida v. Jimeno*, 500 U.S. 248, 250 (1991); *see also* *Platteville Area Apartment Ass’n v. City of Platteville*, 179 F.3d 574, 579 (7th Cir. 1999).

<sup>39</sup> *Platteville*, 179 F.3d at 579.

<sup>40</sup> *See Walter*, 447 U.S. at 656.

<sup>41</sup> *See id.*

<sup>42</sup> *See id.*

has carved out an exception to the general warrant requirement: officers are allowed to seize incriminating evidence in plain view even though outside the scope of the original warrant.<sup>43</sup> Referred to as the plain view doctrine, this is an “exception to the general rule that warrantless searches are presumptively unreasonable.”<sup>44</sup>

The plain view doctrine applies to situations where “the police have a warrant to search a given area for specified objects, and in the course of the search come across some other article of incriminating character.”<sup>45</sup> The Supreme Court clarified the plain view doctrine in its 1990 *Horton v. California* decision.<sup>46</sup> In *Horton*, the warrant authorized a search of the defendant’s house for the proceeds of a robbery, specifically three stolen rings.<sup>47</sup> While executing the search of the defendant’s residence, the police discovered numerous illegal weapons in plain view and seized them.<sup>48</sup> The defendant challenged the admissibility of the weapons by arguing that they were seized outside the scope of the warrant.<sup>49</sup>

The Supreme Court’s analysis focused on the relationship between individual privacy rights and lawful searches.<sup>50</sup> The Court noted that when a warrant is executed, there are two types of rights that may be invaded. First, the search itself compromises a person’s privacy interests.<sup>51</sup> Second, a seizure deprives a person of his or her property rights.<sup>52</sup> The Court reasoned that when the police viewed the weapons, there was no additional or unauthorized privacy violation since the police were already lawfully present in the defendant’s house under the original warrant.<sup>53</sup> Therefore, the plain view doctrine is best

---

<sup>43</sup> See *Horton v. California*, 496 U.S. 128, 135 (1990).

<sup>44</sup> *Id.* at 133.

<sup>45</sup> *Id.* at 135.

<sup>46</sup> See *id.* at 142.

<sup>47</sup> *Id.* at 130–31.

<sup>48</sup> *Id.* at 131.

<sup>49</sup> *Id.*

<sup>50</sup> *Id.* at 133.

<sup>51</sup> *Id.*

<sup>52</sup> *Id.*

<sup>53</sup> *Id.* at 141–42.

viewed as an exception to the protection against illegal seizures.<sup>54</sup> However, the defendant's property rights were not violated because he had no legal right to possess the weapons in the first place, and the illegality of the weapons became immediately apparent.<sup>55</sup> Since a person's privacy or property rights are not violated in these situations, the plain view doctrine comports with the Fourth Amendment.<sup>56</sup>

The Supreme Court formulated three requirements for evidence to be admitted under the plain view doctrine. First, the officer must "be lawfully located in a place from which the object can be plainly seen."<sup>57</sup> Second, the officer must have a lawful right of access to the object.<sup>58</sup> Third, the incriminating character of the item in plain view must be "immediately apparent."<sup>59</sup> If an item is seized when these three requirements are met, it is admissible because the defendant's Fourth Amendment rights have not been violated.<sup>60</sup>

*Horton* was decided in a pre-modern computer era and in the context of traditional physical evidence: guns, drugs, photos, physical documents, and so on.<sup>61</sup> Computer technology as we know it today did not exist; it was relatively primitive and the internet was basically nonexistent.<sup>62</sup> In fact, *Horton* was decided in 1990, the same year that marked the invention of HTML, a programming code that allowed the formation of our modern internet system known as the "world wide web."<sup>63</sup> The question before courts today is whether the pre-computer era plain view doctrine established in *Horton* should be applied to computer searches.

---

<sup>54</sup> *Id.* at 133.

<sup>55</sup> *Id.* at 141–42.

<sup>56</sup> *Id.*

<sup>57</sup> *Id.* at 136–37.

<sup>58</sup> *Id.*

<sup>59</sup> *Id.* (citing *Arizona v. Hicks*, 480 U.S. 321, 326–27 (1987)).

<sup>60</sup> *See id.*

<sup>61</sup> *See generally id.* at 129–50.

<sup>62</sup> *See generally* *Timeline of Computer History*, THE COMPUTER HISTORY MUSEUM, <http://computerhistory.org/timeline/?category=net> (last visited Apr. 30, 2010).

<sup>63</sup> *See id.*

## II. OUR DIGITAL LIVES

Computers permeate nearly every aspect of American life.<sup>64</sup> This has created “an unimaginably vast amount of digital information which is getting vaster ever more rapidly.”<sup>65</sup> And this expansion is not going to stop; in fact, the amount of digital information in the world is predicted to increase tenfold every five years.<sup>66</sup>

Besides the vast sum of digital information that exists, people have created a digital life where formerly physical data have been converted into digital form.<sup>67</sup> For example, “rather than storing images, movies, documents, correspondence, [or] personal records” in physical form, people instead store this information in digital media.<sup>68</sup> However, people are not merely converting files one-for-one from physical to digital.<sup>69</sup> Computer technology has made it easier for people to create an unlimited number of files, images, and documents. For example, it is estimated that Facebook, a social networking website, stores approximately 40 billion user photos.<sup>70</sup>

Additionally, computers often record information even if unintended by the user.<sup>71</sup> For instance, Google records every e-mail sent on its Gmail electronic mail service, as well as any instant messaging communication through Gmail.<sup>72</sup> Additionally, a user’s internet history is recorded on their computer hard drive, which creates a trail of what a person does on his or her computer.<sup>73</sup> A lay computer

---

<sup>64</sup> David J. S. Ziff, Note, *Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant*, 105 COLUM. L. REV. 841, 841 (2005).

<sup>65</sup> *Data, Data Everywhere*, THE ECONOMIST, Feb. 25, 2010.

<sup>66</sup> *Id.*

<sup>67</sup> See RayMing Chang, *Why the Plain View Doctrine Should Not Apply to Digital Evidence*, 12 SUFFOLK J. TRIAL & APP. ADVOC. 31, 35 (2007).

<sup>68</sup> *Id.*

<sup>69</sup> See *Data, Data Everywhere*, *supra* note 65.

<sup>70</sup> *Id.*

<sup>71</sup> See *United States v. Upham*, 168 F.3d 532, 537 (1st Cir. 1999); *Russo v. State*, 228 S.W.3d 779, 790 (Tex. App. 2007).

<sup>72</sup> See *Gmail Privacy Notice*, GMAIL, <http://mail.google.com/mail/help/privacy.html> (last visited Apr. 24, 2010).

<sup>73</sup> See *Upham*, 168 F.3d at 537; *Russo*, 228 S.W.3d at 790.

user might not even know these files exist. But with the proper software, law enforcement can view these files and know what websites a user has visited and what files on his or her computer have been created or opened.<sup>74</sup>

Since criminals are likely to use computers for illegal activity, this digital information is a valuable source of evidence for law enforcement agencies.<sup>75</sup> Today, search warrants frequently include language that authorizes the seizure of computers and other digital devices.<sup>76</sup> However, as more information is stored in digital form, it has become increasingly difficult to separate innocuous files from incriminating files during the search of a computer.<sup>77</sup>

In practice, criminals will hide, mislabel, and bury incriminating evidence among the thousands of innocuous files on a computer.<sup>78</sup> This makes it extremely difficult and time-consuming for law enforcement to discover incriminating evidence.<sup>79</sup> It is unlikely that a criminal will label files on his computer “child pornography,” “debts for illegal drugs,” or “incriminating contact list.”<sup>80</sup> So in order to conduct an effective search, police must open almost every file on a computer.<sup>81</sup> To assist, departments have employed sophisticated software that analyzes and categorizes this immense amount of data into a viewable, workable format.<sup>82</sup>

---

<sup>74</sup> *See id.*

<sup>75</sup> Ziff, *supra* note 64, at 841.

<sup>76</sup> *E.g.*, United States v. Williams, 592 F.3d 511, 515–16 (4th Cir. 2010) (warrant authorizing a search of “[a]ny and all computer systems and digital storage media”); *see also* United States v. Mann, 592 F.3d 779, 780–81 (7th Cir. 2010) (warrant authorizing a search of “video tapes, CD’s or other digital media, computers, and the contents of said computers, tapes, or other electronic media”).

<sup>77</sup> *See* United States v. Gray, 78 F. Supp. 2d 524, 528–29 (E.D. Va. 1999).

<sup>78</sup> *Id.* at 528.

<sup>79</sup> *See id.*

<sup>80</sup> *See id.*; *see also* United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006) (finding that “[c]riminals will do all they can to conceal contraband”).

<sup>81</sup> *See Gray*, 78 F. Supp. 2d at 528 (holding that “[a]lthough care must be taken to minimize the intrusion, records searches require that many, and often all, documents in the targeted location be searched”).

<sup>82</sup> *See* United States v. Mann, 592 F.3d 779, 781 (7th Cir. 2010); United States v. Burgess, 576 F.3d 1078, 1083–84 (10th Cir. 2009); *Gray*, 78 F. Supp. 2d at 527.

Federal and state courts across the United States are more frequently confronted with cases involving digital searches and seizures.<sup>83</sup> Without clear guidance from the Supreme Court, the federal circuits have approached this situation differently. For example, the Tenth Circuit has held that a subjective intent standard should be applied when determining whether digital evidence is admissible.<sup>84</sup> Further, the Ninth Circuit has advocated abandoning the plain view doctrine altogether in digital evidence cases, and instead has sought to adopt a multistep prophylactic approach to prevent overly broad computer searches.<sup>85</sup> In contrast, the Seventh Circuit, as well as the majority of other federal circuits, has continued to apply traditional Fourth Amendment doctrine to digital evidence cases.<sup>86</sup>

The most prudent approach for courts to follow in future digital evidence cases is to adhere to traditional Fourth Amendment doctrine. Courts should determine whether the search was reasonable, whether the evidence fell within the plain view doctrine, and whether the warrant met the particularity requirement. Computer searches raise significant privacy concerns, and courts should be aware of the differences between physical and digital evidence. However, it makes more sense to incrementally develop the contours of the plain view doctrine than to prematurely abandon it and develop a completely new test or framework. As more cases come before the courts, the contours of Fourth Amendment doctrine will incrementally develop so that individuals' privacy and property rights will remain protected.

---

<sup>83</sup> See *United States v. Williams*, 592 F.3d 511, 514 (4th Cir. 2010); *Mann*, 592 F.3d at 782; *United States v. Carey*, 172 F.3d 1268, 1271 (10th Cir. 1999); *Gray*, 78 F. Supp. 2d at 528.

<sup>84</sup> See *Carey*, 172 F.3d at 1273.

<sup>85</sup> See *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1006 (9th Cir. 2009).

<sup>86</sup> See generally *Williams*, 592 F.3d 511; *Mann*, 592 F.3d at 785; *United States v. Burgess*, 576 F.3d 1078 (10th Cir. 2009); *United States v. Miranda*, 325 Fed. App'x 858 (11th Cir. 2009); *United States v. Turner*, 169 F.3d 84 (1st Cir. 1999); *United States v. Henson*, 848 F.2d 1374 (6th Cir. 1988).

### III. THE FEDERAL CIRCUITS' APPROACHES TO DIGITAL EVIDENCE CASES

Although *United States v. Mann* is the focus of this Note, the Seventh Circuit's analysis heavily relies on two previous opinions from the Ninth and Tenth Circuits. In order to understand the *Mann* decision and why the traditional Fourth Amendment doctrine is the proper standard for courts to follow, it is important to discuss the facts and analyses that the Ninth and Tenth Circuits applied to their respective digital evidence cases.

#### A. *The Tenth Circuit's Subjective Standard*

In 1999, the Tenth Circuit decided *United States v. Carey*, one of the first federal appeal level decisions to examine Fourth Amendment search and seizure doctrine in the context of digital evidence.<sup>87</sup> The case stemmed from an at-home arrest of the defendant for the sale and possession of cocaine.<sup>88</sup> The police observed a bong in plain view when they arrested Carey in his apartment.<sup>89</sup> Carey then consented to a search of his apartment by signing a written consent form.<sup>90</sup> The police discovered and seized illegal drugs as well as two computers believed to contain more evidence of drug trafficking.<sup>91</sup>

After the computers were seized, a magistrate issued a warrant authorizing a search of both computers for "names, telephone numbers, ledger receipts, addresses, and other *documentary evidence* pertaining to the sale and distribution of controlled substances."<sup>92</sup> The detective who conducted the search first manually inspected the computer and entered keyword searches such as "money, accounts, [or] people" to locate files with these types of filenames.<sup>93</sup> However,

---

<sup>87</sup> See 172 F.3d at 1273.

<sup>88</sup> *Id.* at 1270.

<sup>89</sup> *Id.*

<sup>90</sup> *Id.*

<sup>91</sup> *Id.*

<sup>92</sup> *Id.* (emphasis added).

<sup>93</sup> *Id.* at 1271.

this method did not uncover any files related to drugs.<sup>94</sup> The detective continued to explore the directories and discovered hundreds of JPG image files—the first one he opened was child pornography.<sup>95</sup> He then proceeded to save 240 JPG image files to nineteen disks and opened a sampling of five to seven images from each disk, most of which were child pornography.<sup>96</sup>

At trial, the defendant moved to suppress all of the child pornography.<sup>97</sup> During the hearing on the motion to suppress, the detective testified that once he discovered the first image of child pornography, he diverted from his original search for drug activity and began a second search for child pornography.<sup>98</sup>

The defendant argued that the detective exceeded the scope of the warrant, which only authorized a search for “documentary evidence,” not image files.<sup>99</sup> The government argued that the images were admissible because they were properly seized under the plain view doctrine.<sup>100</sup>

The Tenth Circuit’s analysis noted that “[t]he essential inquiry when faced with challenges under the Fourth Amendment is whether the search or seizure was reasonable.”<sup>101</sup> The warrant authorized a search of both computers for files with “names, telephone numbers, ledgers, receipts, addresses, and other *documentary evidence* pertaining to the sale and distribution of controlled substances.”<sup>102</sup> The court narrowly interpreted the warrant’s language to only authorize a search for “documentary files,” such as Word, Excel, or Adobe PDF documents that would contain text-based information.<sup>103</sup> Reasoning

---

<sup>94</sup> *Id.*

<sup>95</sup> *Id.*

<sup>96</sup> *Id.*

<sup>97</sup> *Id.*

<sup>98</sup> *Id.*

<sup>99</sup> *Id.* at 1272.

<sup>100</sup> *Id.*

<sup>101</sup> *Id.* (quoting *O’Rourke v. City of Norman*, 875 F.2d 1465, 1472 (10th Cir. 1989)).

<sup>102</sup> *Id.* at 1272–73 (emphasis added).

<sup>103</sup> *See id.*; *United States v. Burgess*, 576 F.3d 1078, 1093 (10th Cir. 2009) (discussing various computer file types and extensions).

that image files are not “documentary” in nature, the court held that the image files found in the defendant’s computer were not within the scope of the warrant.<sup>104</sup> Therefore, the detective exceeded the scope of the warrant by downloading and opening the JPG images.<sup>105</sup> And since the detective could not lawfully open or view any image files during his search, the child pornography did not satisfy the requirements of the plain view doctrine.<sup>106</sup>

The Tenth Circuit also held that the detective should have known that the content of the image files was outside the scope of the warrant prior to opening them because “most featured a sexually suggestive title.”<sup>107</sup> Further, even if the officer did not know the content of the first file, the detective should have known after opening it that the other files in the directory were likely to be child pornography as well.<sup>108</sup> At this point, the detective should have stopped his search and obtained a second warrant to search for child pornography.<sup>109</sup> There would have been probable cause for a second warrant based on the one known child pornography file, as well as the other sexually suggestive file names.<sup>110</sup>

The court’s primary basis for holding the image files inadmissible rested on the detective’s own admission at the hearing.<sup>111</sup> The court found it “plainly evident [that] each time he opened a subsequent JPG file, he expected to find child pornography and not material related to drugs.”<sup>112</sup> This departure marked the end point of the original search and constituted a second, unauthorized, and illegal search of the defendant’s computer.<sup>113</sup> By exceeding the scope of the

---

<sup>104</sup> *Carey*, 172 F.3d at 1272–73.

<sup>105</sup> *Id.*

<sup>106</sup> *See id.*; *see also* *Horton v. California*, 496 U.S. 128, 137 (1990) (holding that the plain view doctrine requires that the officer must “be lawfully located in a place from which the object can be plainly seen”).

<sup>107</sup> *Carey*, 172 F.3d at 1274.

<sup>108</sup> *Id.*

<sup>109</sup> *Id.* at 1276 (Baldock, J., concurring).

<sup>110</sup> *Id.* at 1276–77.

<sup>111</sup> *See id.* at 1273 (majority opinion).

<sup>112</sup> *Id.*

<sup>113</sup> *See id.*

warrant, the detective's search was unreasonable, and any fruits of that search were inadmissible.<sup>114</sup>

The Tenth Circuit explicitly stated that *Carey* did not involve the plain view doctrine.<sup>115</sup> Instead, the court's analysis centered on the subjective intent of the officer who admitted that he diverged from his original search and began a second search for more evidence of child pornography.<sup>116</sup> In contrast, if the warrant had authorized a search for "image files" for evidence relating to drug trafficking, the court may have come to a different conclusion. Under this alternative scenario, the plain view doctrine would apply since the detective would be in a lawful position to open the image files, and the criminality of the child pornography would be immediately apparent.<sup>117</sup>

Subsequent courts and scholars have interpreted *Carey* differently. The *Carey* decision goes to great lengths to state that its ruling was fact-specific and that it was not addressing the broad use of the plain view doctrine in digital evidence cases.<sup>118</sup> Ten years after *Carey*, the Tenth Circuit highlighted its limitation in *United States v. Burgess*.<sup>119</sup> In *Burgess*, a police detective was executing a search of the defendant's computer for evidence related to illegal drug activity.<sup>120</sup> The detective inadvertently discovered child pornography; however, he stopped his search after viewing the first image and obtained a second warrant to search for child pornography.<sup>121</sup> He then renewed his search and discovered approximately 70,000 images of child pornography.<sup>122</sup> The district court held that these images were properly seized and admissible.<sup>123</sup>

---

<sup>114</sup> *See id.*

<sup>115</sup> *Id.* ("Although the question of what constitutes 'plain view' in the context of computer files is intriguing and appears to be an issue of first impression for this court, and many others, we do not need to reach it here.").

<sup>116</sup> *See id.* at 1272–73.

<sup>117</sup> *See id.*; *see also* *Horton v. California*, 496 U.S. 128, 136–37 (1990).

<sup>118</sup> *See Carey*, 172 F.3d. at 1273.

<sup>119</sup> 576 F.3d 1078, 1092 (10th Cir. 2009).

<sup>120</sup> *Id.* at 1083–84.

<sup>121</sup> *Id.* at 1084.

<sup>122</sup> *Id.*

<sup>123</sup> *Id.* at 1095.

The Tenth Circuit distinguished the *Carey* and *Burgess* holdings on factual grounds. First, the officer in *Burgess* did not diverge from his original search and begin a second unauthorized search as the detective did in *Carey*.<sup>124</sup> Second, the *Burgess* decision reiterated that *Carey* was fact-dependent and limited.<sup>125</sup> *Carey* was an easily decided case because the subjective intent of the detective so clearly exceeded the scope of the warrant.<sup>126</sup> However, this limits *Carey*'s application in cases where the subjective intent of the officer is not so clear.<sup>127</sup>

Some legal scholars who advocate an abandonment of the plain view doctrine use *Carey* as a jumping-off point. For example, Orin Kerr of the George Washington University Law School argues that *Carey* adopts a new subjective standard when determining the reasonableness of a search.<sup>128</sup> Kerr argues that this subjective approach “offers one significant advantage over the existing objective test: it turns the emphasis from a question judges are poorly equipped to answer (the reasonableness of a forensic step) to a question judges are better positioned to answer (witness credibility).”<sup>129</sup> Kerr attempts to discredit the knowledge, wisdom, and skill of all judges by arguing that the process of computer searches is “too complex and fluid” for judges to grasp.<sup>130</sup>

Nevertheless, a subjective standard raises several concerns that ultimately lead to its impracticability. First, any inquiry into the subjective intent of the executing officer goes directly against Supreme Court precedent.<sup>131</sup> In *Horton*, the Supreme Court based this conclusion on practical concerns by noting, “evenhanded law enforcement is best achieved by the application of objective standards of conduct, rather than standards that depend upon the subjective state

---

<sup>124</sup> *Id.* at 1092.

<sup>125</sup> *Id.*

<sup>126</sup> *See id.*

<sup>127</sup> *See id.*

<sup>128</sup> Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 578 (2005); *see also* Chang, *supra* note 67, at 46–50.

<sup>129</sup> Kerr, *supra* note 128, at 578.

<sup>130</sup> *See id.*

<sup>131</sup> *See Horton v. California*, 496 U.S. 128, 138 (1990).

of mind of the officer.”<sup>132</sup> The scope of a search warrant is “defined by the object of the search and the places in which there is probable cause to believe that it may be found.”<sup>133</sup> In the absence of any Supreme Court case law supporting a deviation from general Fourth Amendment precedent, courts should not adopt a new subjective intent standard in digital evidence cases.

Second, a subjective standard would induce testifying police officers to perjure themselves in order to admit improperly seized computer files. For evidence of this temptation, one needs to look no further than the Tenth Circuit’s *United States v. Carey* decision.<sup>134</sup> During the hearing on the motion to suppress, Detective Lewis at first stated that he knew the files likely contained child pornography.<sup>135</sup> He knew he was exceeding the scope of the warrant, stating, “that question did arise, and my captain took care of [the issue] through the county attorney’s office.”<sup>136</sup> After further questioning by the government, Detective Lewis later recanted his previous statement and asserted that he did not really know the contents of the JPG files before opening them.<sup>137</sup> Although the judge rejected his later testimony, this example illustrates the perverse incentives that would confront testifying police officers if courts adopted a subjective intent standard.

Just as the decision itself stated, *Carey* should be read narrowly.<sup>138</sup> Although it can be argued that the Tenth Circuit had the opportunity to address the application of the plain view doctrine to digital evidence, the court chose not to.<sup>139</sup> Instead, the Tenth Circuit applied a reasonableness standard to determine whether the detective’s

---

<sup>132</sup> *Id.*; see also *Whren v. United States*, 517 U.S. 806, 813 (1996) (holding that “[s]ubjective intentions play no role in ordinary, probable-cause Fourth Amendment analysis”).

<sup>133</sup> *United States v. Ross*, 456 U.S. 798, 824 (1982).

<sup>134</sup> 172 F.3d 1268, 1271 (9th Cir. 1999).

<sup>135</sup> *Id.*

<sup>136</sup> *Id.*

<sup>137</sup> *Id.*

<sup>138</sup> *Id.* at 1276.

<sup>139</sup> See *Chang*, *supra* note 67, at 48.

search comported with the protections of the Fourth Amendment, which it did not.<sup>140</sup>

### *B. The Ninth Circuit's Prophylactic Test*

While the Tenth Circuit hinted at a slight divergence from traditional Fourth Amendment doctrine, the Ninth Circuit has directly abandoned it.<sup>141</sup> In 2009, the Ninth Circuit decided *United States v. Comprehensive Drug Testing, Inc.* (“CDT”), a case concerning the highly-publicized seizure of computer files holding the steroid test results of Major League Baseball players.<sup>142</sup>

The Major League Baseball Players Association (“the Players”) and Major League Baseball (“MLB”) had entered into an agreement where all players would be drug tested.<sup>143</sup> Both sides agreed that the results would be strictly confidential and were intended only to allow the MLB to determine the degree of steroid use among athletes.<sup>144</sup> Comprehensive Drug Testing, Inc. (“CDT”) administered, analyzed, and stored the test results.<sup>145</sup>

The federal government suspected that the Bay Area Lab Cooperative (“Balco”) illegally distributed steroids to baseball players.<sup>146</sup> The government established probable cause to seize the test results of ten players, and a magistrate issued a search warrant authorizing such seizure from CDT.<sup>147</sup> Federal agents executed the warrant and seized not only the records of the ten players, but also reviewed the records of hundreds of other players who had been

---

<sup>140</sup> See *Carey*, 172 F.3d at 1272.

<sup>141</sup> See *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1006–07 (9th Cir. 2009); *Carey*, 172 F.3d at 1276.

<sup>142</sup> See 579 F.3d at 993.

<sup>143</sup> *Id.*

<sup>144</sup> *Id.*

<sup>145</sup> *Id.*

<sup>146</sup> *Id.*

<sup>147</sup> *Id.*

tested.<sup>148</sup> CDT and the Players moved to have the government return the test results that were improperly seized.<sup>149</sup>

The Ninth Circuit analogized the facts in *CDT* to a previous Ninth Circuit decision, *United States v. Tamura*.<sup>150</sup> In *Tamura*, the government seized thousands of paper records relating to the defendant's business.<sup>151</sup> Instead of separating innocuous files from incriminating ones on site, the government seized all of the files and planned to later separate them.<sup>152</sup> *Tamura* argued that the scope of the search was too broad and resulted in a wholesale seizure of documents not mentioned in the warrant.<sup>153</sup> The government argued that this broad seizure was necessary because "the documents were intermingled and it was difficult to separate the described documents from the irrelevant ones" on site.<sup>154</sup> The Ninth Circuit held a search is restricted to specifically enumerated items in the warrant.<sup>155</sup> By seizing such a large amount of unrelated files, the government's search and seizure was significantly intrusive and violated Fourth Amendment principles.<sup>156</sup> The *CDT* court equated the wholesale seizure of business files in *Tamura* to the federal agents in *CDT* who

---

<sup>148</sup> *Id.*

<sup>149</sup> *Id.* at 993–94.

<sup>150</sup> *Id.* at 995–96.

<sup>151</sup> *United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982).

<sup>152</sup> *Id.*

<sup>153</sup> *Id.*

<sup>154</sup> *Id.*

<sup>155</sup> *Id.* ("As a general rule, in searches made pursuant to warrants only the specifically enumerated items may be seized.")

<sup>156</sup> *Id.*; *but see* *United States v. Henson*, 848 F.2d 1374, 1383–84 (6th Cir. 1988) (holding that in the context of a computer search "it was inevitable that the officers would seize documents that were not relevant to the proceedings at hand. We do not think it is reasonable to have required the officers to sift through the large mass of documents and computer files found in the Hensons' office, in an effort to segregate those few papers that were outside the warrant."); *United States v. Turner*, 13 F. Supp. 2d 574, 583 (D. Vt. 1988) ("Often it is simply impractical to search a computer at the search site because of the time and expertise required to unlock all sources of information.").

seizure from CDT of the test results of hundreds of players not authorized by the warrant.<sup>157</sup>

Much of the court's reasoning rested on the fact that "[t]he Government demonstrated a callous disregard for the rights of those persons whose records were seized and searched outside the warrant."<sup>158</sup> The warrant contained restrictions on how the seized data was to be handled; however, federal agents explicitly disregarded these limitations.<sup>159</sup> For example, the warrant specified that neutral computer personnel, not investigating agents, were supposed to segregate relevant from irrelevant files.<sup>160</sup> Nevertheless, the federal agents immediately made copies of all files and examined the test results themselves.<sup>161</sup> At hearing, an Assistant United States Attorney even stated that a federal agent "briefly [perused the file] to see if there was anything above and beyond that which was authorized for seizure in the initial warrant."<sup>162</sup>

Instead of seeing the federal agents' actions as a single act of malfeasance, the Ninth Circuit concluded "that such over-seizing is an inherent part of the electronic search process" and will become a more prevalent problem with digital evidence.<sup>163</sup> In order to protect against this danger, the Ninth Circuit prescribed a five-part test that warrant-issuing magistrates should follow in digital evidence cases: (1) reliance on the plain view doctrine must be waived in digital evidence cases; (2) an independent third party must review, segregate, and redact files before being given to investigators; (3) warrants must disclose the risks of destruction of information and prior efforts to seize that information; (4) the government's search protocol must be designed to uncover only information for which it has probable cause; and (5) the government must either destroy or return evidence outside

---

<sup>157</sup> See *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 997–99 (9th Cir. 2009).

<sup>158</sup> *Id.* at 997.

<sup>159</sup> *Id.* at 995–97.

<sup>160</sup> *Id.* at 995–96.

<sup>161</sup> *Id.* at 996–97.

<sup>162</sup> *Id.* at 1010 (Callahan, J., concurring in part and dissenting in part).

<sup>163</sup> *Id.* at 1006 (majority opinion).

the scope of the warrant.<sup>164</sup> The Ninth Circuit was reluctant to call this a test and instead offered it as a “useful tool for the future.”<sup>165</sup> However, at least one decision from the Northern District of California has treated the *CDT* test as the new Fourth Amendment standard to apply in the Ninth Circuit.<sup>166</sup>

Although such a prophylactic approach may seem attractive, the Ninth Circuit’s holding in *CDT* is overbroad and unnecessary, and it misinterprets the primary issue of the case. What distinguishes *CDT* from the other cases is the fact that the search was unlawful because of the overbroad and intrusive actions of the federal agents conducting it.<sup>167</sup> The majority decision itself recognized that the seizure at issue was an “obvious case of deliberate overreaching by the government in an effort to seize data as to which it lacked probable cause.”<sup>168</sup>

The Ninth Circuit could have concluded that the intrusive and illegal actions by the federal agents constituted a single event. Instead, the court broadly concluded that such “over-seizing is an inherent part of the electronic search process.”<sup>169</sup> As discussed in Judge Callahan’s concurrence and dissent, “the majority’s prescriptions go significantly beyond what is necessary for it to resolve this case.”<sup>170</sup> Judge Callahan argues that instead of casting traditional Fourth Amendment doctrine aside, “the prudent course would be to allow [its] contours . . . to develop incrementally through the normal course of fact-based case adjudication.”<sup>171</sup> The Ninth Circuit would have reached the same result if it had applied traditional Fourth Amendment doctrine.<sup>172</sup> The government’s seizure would have grossly exceeded the scope of the

---

<sup>164</sup> *Id.*

<sup>165</sup> *Id.* at 1007.

<sup>166</sup> *United States v. Cerna*, No. CR 08-0730 WHA, 2009 WL 5125920, at \*7 (N.D. Cal. Dec 21, 2009).

<sup>167</sup> *See Comprehensive Drug Testing, Inc.*, 579 F.3d at 997.

<sup>168</sup> *Id.* at 1000.

<sup>169</sup> *Id.* at 1006.

<sup>170</sup> *Id.* at 1012 (Callahan, J., concurring in part and dissenting in part).

<sup>171</sup> *Id.* at 1013.

<sup>172</sup> *See id.* at 1012–13.

warrant, the search would have been determined to be unreasonable, and the test results of the other players would have been suppressed.<sup>173</sup>

In the short time since the *CDT* decision, criminal defendants have attempted to persuade other courts to follow this new standard.<sup>174</sup> However, most courts outside of the Ninth Circuit have been hesitant to adopt the prophylactic *CDT* test.<sup>175</sup> The Seventh Circuit in *United States v. Mann* has been the only federal appellate court to address *CDT* to date, and it was skeptical of *CDT*'s overbroad approach.<sup>176</sup> Instead, the Seventh Circuit aligned its decision closer to Judge Callahan's *CDT* dissent and sought to allow traditional Fourth Amendment doctrine to evolve in digital evidence cases.<sup>177</sup>

Federal district and state courts have suggested that the *CDT* standard "creates more problems than it solves"<sup>178</sup> and is only an optional, useful tool for the future.<sup>179</sup> These courts instead focus on the specific facts in *CDT* that involved egregious conduct by government agents.<sup>180</sup> Whereas most courts have viewed egregious police misconduct to be the exception, the Ninth Circuit appears to reason that police misconduct will be the rule in future digital evidence

---

<sup>173</sup> See *id.* at 995–97 (majority opinion). This distinction is very similar to the Tenth Circuit's *Carey* decision. Both *Carey* and *CDT* involved situations where the executing officers greatly exceeded the scope of the warrant, thereby making their searches unreasonable and providing grounds to suppress the evidence. The Ninth and Tenth Circuits adopted new frameworks for digital evidence cases, even though the divergence was unnecessary to resolve each case.

<sup>174</sup> See, e.g., *United States v. Sedaghaty*, Cr. No. 05-60008-HO, 2010 WL 1490306, at \*5 (D. Or. Apr. 13, 2010); *United States v. Wilbur*, No. CR09-191 MJP, 2010 WL 519735, at \*16 (W.D. Wash. Feb. 4, 2010); *United States v. Kim*, 677 F. Supp. 2d 930, 946 (S.D. Tex. 2009).

<sup>175</sup> See *id.*

<sup>176</sup> See *United States v. Mann*, 592 F.3d 779, 785–86 (7th Cir. 2010).

<sup>177</sup> *Id.* at 785. The details of *United States v. Mann* will be discussed in further detail *infra*.

<sup>178</sup> *United States v. Farlow*, No. CR-09-38-B-W, 2009 WL 4728690, at \*6 n.3 (D. Me. Dec. 3, 2009) (arguing that the new standard is unnecessary because "the traditional sanction for police misconduct of this sort remains exclusion of evidence").

<sup>179</sup> See *United States v. King*, CR No. 09-00207 DAE, 2010 WL 727981, at \*25 (D. Haw. Mar. 1, 2010).

<sup>180</sup> *Farlow*, 2009 WL 4728690, at \*6 n.3.

cases.<sup>181</sup> Under this line of thinking, *CDT*'s expansive pre-issuance procedures are justified. However, it is extremely pessimistic to assume that all law enforcement officials will be as overzealous as the federal agents in *CDT* when conducting a digital search.<sup>182</sup>

Besides, there are existing remedies within the law that deter law enforcement from exceeding the scope of a warrant or otherwise acting unlawfully. First, the exclusionary rule deters officers from acting unlawfully while executing a warrant.<sup>183</sup> The exclusionary rule prohibits the admission of any evidence at trial that was obtained from an illegal search or seizure.<sup>184</sup> This rule incentivizes police officers to conform their conduct to the requirements of the law since police officers presumably want seized evidence to be admitted in court.<sup>185</sup> Second, if the exclusionary rule does not deter an officer, there is a civil remedy available under 42 U.S.C. § 1983<sup>186</sup> for police violations of constitutional rights.<sup>187</sup> § 1983 provides redress to any citizen whose constitutional rights are violated by any person acting under color of law.<sup>188</sup> Therefore, a citizen would have a meritorious § 1983 suit if a police officer violated her Fourth Amendment rights by conducting an unreasonable search and seizure.<sup>189</sup> These two existing

---

<sup>181</sup> *See id.*

<sup>182</sup> *See id.* (“There is no evidence that police disobedience of search warrant limitations is so widespread to compel such onerous pre-issuance procedures, and at the very least the more traditional remedies should be tried first.”).

<sup>183</sup> *See Elkins v. United States*, 364 U.S. 206, 217 (1960) (holding the purpose of the exclusionary rule is “to deter—to compel respect for the constitutional guaranty . . . by removing the incentive to disregard it”).

<sup>184</sup> *See Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 391–92 (1920).

<sup>185</sup> *See Elkins*, 364 U.S. at 217.

<sup>186</sup> 42 U.S.C. § 1983 (“Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress.”).

<sup>187</sup> *Hudson v. Michigan*, 547 U.S. 586, 597–98 (2006).

<sup>188</sup> *Monell v. Dep’t of Soc. Servs. of N.Y.C.*, 436 U.S. 658, 690 (1978); *Monroe v. Pape*, 365 U.S. 167, 172 (1961).

<sup>189</sup> *See id.*

remedies provide sufficient protection to individuals from the unreasonable or overzealous searches over which the Ninth Circuit was concerned in *CDT*, thereby making the prophylactic measures overbroad and unnecessary.<sup>190</sup>

The Ninth Circuit was presented with a factual scenario where the federal agents' actions were clearly egregious and exceeded the scope of the warrant.<sup>191</sup> That in and of itself is enough to suppress the test results because it constituted an unreasonable search.<sup>192</sup> Instead of issuing a narrow ruling, the Ninth Circuit adopted an overly broad approach in an attempt to prevent future police misconduct.<sup>193</sup> The proper approach would have been to rely on the traditional Fourth Amendment principles of reasonableness, the particularity requirement, and the plain view doctrine. Although digital evidence cases present new issues and problems, the contours of these doctrines should be allowed to develop incrementally as different factual scenarios come before courts.

### *C. The Seventh Circuit Weighs In: United States v. Mann*

On January 20, 2010, the Seventh Circuit weighed in on this issue in *United States v. Mann*.<sup>194</sup> The *Mann* decision shares many similarities with the hypothetical situation posed in the introduction of this Note. However, the facts of *Mann* require further development because of certain significant differences. In 2007, Matthew Mann worked as a lifeguard instructor for the Red Cross in Tippecanoe County, Indiana.<sup>195</sup> He installed a video camera in the women's locker room in order to record women changing their clothes.<sup>196</sup> However, in addition to videotaping women in the locker room, he recorded

---

<sup>190</sup> See *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1006 (9th Cir. 2009).

<sup>191</sup> See *id.* at 997.

<sup>192</sup> See *Illinois v. McArthur*, 531 U.S. 326, 330 (2001).

<sup>193</sup> See *Comprehensive Drug Testing, Inc.*, 579 F.3d at 1006.

<sup>194</sup> 592 F.3d 779 (7th Cir. 2010).

<sup>195</sup> *Id.* at 780.

<sup>196</sup> *Id.*

himself installing the camera.<sup>197</sup> One of his female students discovered the camera, played the tape for herself, and recognized Mann.<sup>198</sup> She contacted the police department and turned over the video camera and videotape.<sup>199</sup>

Days later, the police obtained a warrant authorizing a search of Mann's residence for "video tapes, CD's or other digital media, computers, and the contents of said computers, tapes, or other electronic media, to search for images of women in locker rooms or other private areas."<sup>200</sup> The police executed the warrant and seized two desktop computers, a laptop, and an external hard drive.<sup>201</sup> The next day, Mann was arrested for voyeurism in violation of Indiana law.<sup>202</sup>

Two months later, a police detective conducted a search of Mann's computers.<sup>203</sup> He began by creating an exact copy of the computer hard drives in order to prevent the data from being altered or destroyed.<sup>204</sup> The detective searched the content of the hard drives using a software program, known as a "forensic tool kit" (FTK).<sup>205</sup> The FTK software examines every file on the computer and then displays an overview screen with thumbnail images of every image, video, and document on the computer.<sup>206</sup>

The FTK software also flags computer files using a "KFF Alert," or Known File Filter.<sup>207</sup> The software cross-references all filenames on the computer with a national registry consisting of illegal files previously seized by other law enforcement agencies.<sup>208</sup> Any

---

<sup>197</sup> *Id.*

<sup>198</sup> *Id.*

<sup>199</sup> *Id.*

<sup>200</sup> *Id.* at 780–81.

<sup>201</sup> *Id.* at 781.

<sup>202</sup> *Id.*; see IND. CODE ANN. § 35-45-4-5(a)(2)(b)(1) (2004).

<sup>203</sup> *Mann*, 592 F.3d at 781.

<sup>204</sup> *Id.*

<sup>205</sup> *Id.*

<sup>206</sup> *Id.*

<sup>207</sup> *Id.*

<sup>208</sup> *Id.* The original warrant authorized the detective to search the computer for any files that might contain voyeurism. At the very least, this authorized the detective to read the file names on the computer. The KFF cross-reference does not

matches are flagged with a “KFF Alert.”<sup>209</sup> Most files from the national directory are child pornography.<sup>210</sup>

While searching Mann’s computers, the detective discovered photos of girls taken from a high school locker room, child pornography, and a story about a swim coach masturbating while watching young girls swim, possibly written by Mann.<sup>211</sup> No files were flagged by the KFF Alert during this first search.<sup>212</sup>

Two months after the first search,<sup>213</sup> the detective searched Mann’s external hard drive using the same software program.<sup>214</sup> Four files on the hard drive were flagged with a KFF Alert, indicating that the files were likely child pornography.<sup>215</sup> The detective opened every file on the hard drive, including the four KFF Alert files, which were indeed child pornography.<sup>216</sup> He also found two more videos from a high school locker room.<sup>217</sup>

Mann moved to suppress the child pornography by arguing that the detective exceeded the scope of the warrant, but the district court

---

go beyond what the officer could do with his own eyes. Therefore, the KFF Alert does not create an additional second search for Fourth Amendment purposes.

<sup>209</sup> *Id.*

<sup>210</sup> *Id.*

<sup>211</sup> *Id.*

<sup>212</sup> *Id.*

<sup>213</sup> *Id.* at 781. The Seventh Circuit commented that it was “problematic that nearly two months elapsed before Detective Huff began his search of the Western Digital hard drive despite having found child pornography on the Dell laptop.” *Id.* at 786. The court was reluctant to specify a proper time frame and only alluded to a potential constitutional violation at some point. *See id.* Other courts ruling on this specific issue have given police departments great flexibility due to practical considerations, such as time constraints and limited resources. The determining factor has been whether the police officers were acting in good faith to stay within the boundaries of the warrant. *See generally* United States v. Syphers, 296 F. Supp. 2d 50, 59 (D. N.H. 2003); United States v. Yung, 786 F. Supp. 1561, 1569 (D. Kan. 1992); *but see* United States v. Brunette, 76 F. Supp. 2d 30, 42 (D. Me. 1999) (holding that a search was unlawful when it was executed sixty-two days after the seizure of the computer and the warrant was only valid for sixty days).

<sup>214</sup> *Mann*, 592 F.3d at 781.

<sup>215</sup> *Id.*

<sup>216</sup> *Id.*

<sup>217</sup> *Id.*

denied his motion.<sup>218</sup> The court reasoned that the warrant authorized the detective to examine any files on the computer that may have involved voyeurism, and that the detective never abandoned his search for voyeurism when he inadvertently discovered the child pornography.<sup>219</sup> Although outside the scope of the warrant, the district court held that the child pornography was admissible under the plain view doctrine.<sup>220</sup> Mann then entered a conditional guilty plea to one count of possession of child pornography and appealed the district court's denial of his motion to suppress.<sup>221</sup>

Mann's appeal rested on three arguments. First, Mann argued that by utilizing the FTK software, the detective's search was unreasonable because it exceeded the scope of the warrant.<sup>222</sup> Mann interpreted the warrant to be restrictive—only authorizing a search for “images of women in locker rooms and other private places.”<sup>223</sup> Mann argues that he was subjected to a general search since every file on his computer was examined by the software.<sup>224</sup> The Seventh Circuit rejected this argument based on practical concerns, reasoning that these types of software programs are essential tools for law enforcement since digital files “could be nearly anywhere on the computers.”<sup>225</sup> The court distinguished physical searches from digital searches by noting, “[u]nlike a physical object that can be immediately identified as responsive to the warrant or not, computer files may be manipulated to hide their true contents.”<sup>226</sup> Therefore the court held that it was reasonable for the detective to both use the FTK software program and briefly examine all files on the computer in order to determine their contents.<sup>227</sup>

---

<sup>218</sup> *Id.* at 781–82.

<sup>219</sup> *Id.*

<sup>220</sup> *See id.* at 782.

<sup>221</sup> *Id.*

<sup>222</sup> *Id.*

<sup>223</sup> *Id.*

<sup>224</sup> *See id.*

<sup>225</sup> *Id.*

<sup>226</sup> *Id.*

<sup>227</sup> *See id.* at 782–83.

Second, relying on the Tenth Circuit's recent decision in *United States v. Carey*, Mann argued that the detective turned the specific search into a general search by looking for evidence of crimes unrelated to voyeurism.<sup>228</sup> The Seventh Circuit rejected this argument because it distinguished the facts in *Mann* from those in *Carey*.<sup>229</sup> First, the warrant in *Carey* only authorized a search for documentary evidence (i.e., Word or Excel documents), but the detective unlawfully extended his search by opening image files.<sup>230</sup> In contrast, the *Mann* warrant authorized the detective to examine any image file that may have been related to voyeurism.<sup>231</sup> Therefore, the search was reasonable because the detective in *Mann* opened files within the scope of the warrant.<sup>232</sup>

The *Carey* and *Mann* facts can be further distinguished by scrutinizing the subjective intent of the officer executing the warrant.<sup>233</sup> The officer in *Carey* admitted that after he discovered the first image of child pornography, he diverged from his original search for evidence of drug dealing.<sup>234</sup> The officer's second, unauthorized search for child pornography exceeded the scope of the warrant and was therefore unreasonable.<sup>235</sup> In contrast, the detective in *Mann* testified that he "continued to look for items with voyeurism" and only made notations where he inadvertently discovered child

---

<sup>228</sup> *Id.* at 783.

<sup>229</sup> *Id.* at 783–85.

<sup>230</sup> *Id.* at 783.

<sup>231</sup> *Id.* The warrant authorized a search for "video tapes, CD's or other digital media, computers, and the contents of said computers, tapes, or other electronic media, to search for images of women in locker rooms or other private areas." *Id.* at 780–81.

<sup>232</sup> *Id.* at 783–84.

<sup>233</sup> *Id.* at 784. The Supreme Court has held that the subjective intent of the executing officer is irrelevant in determining whether the search was reasonable. *See Whren v. United States*, 517 U.S. 806, 813 (1996) (holding "[s]ubjective intentions play no role in ordinary, probable-cause Fourth Amendment analysis"). Despite this, the Seventh Circuit used this factual difference to further distinguish the *Mann* decision since *Carey* so heavily relied on subjective intent in reaching its holding.

<sup>234</sup> *United States v. Carey*, 172 F.3d 1269, 1273 (10th Cir. 1999).

<sup>235</sup> *See id.*

pornography.<sup>236</sup> The Seventh Circuit held that his search was reasonable since he never abandoned his search for evidence of voyeurism.<sup>237</sup>

Mann's third argument urged the Seventh Circuit to adopt the prophylactic rules advocated by the Ninth Circuit in *United States v. Comprehensive Drug Testing, Inc.*<sup>238</sup> The Seventh Circuit rejected this preventative approach because it was overbroad.<sup>239</sup> The Seventh Circuit recognized that "there is nothing in the Supreme Court's case law (or the Ninth Circuit's for that matter) counseling the complete abandonment of the plain view doctrine in digital evidence cases."<sup>240</sup> Instead, the proper approach "would be to allow the contours of the plain view doctrine to develop incrementally through the normal course of fact-based case adjudication."<sup>241</sup> The court saw the Ninth Circuit's approach as diverging from Fourth Amendment precedent, when there is no indication or need to do so.<sup>242</sup>

The Seventh Circuit based its holding on the traditional principles of Fourth Amendment analysis. First, the court held that warrants must "describe with particularity the things to be seized and that searches are narrowly tailored to uncover only those things described."<sup>243</sup> The *Mann* court did not abandon the plain view doctrine and emphasized that reasonableness is the most appropriate standard to apply when determining whether a search violated the protections of the Fourth Amendment.<sup>244</sup>

Applying a reasonableness standard, the court affirmed the district court's ruling with one exception.<sup>245</sup> The Seventh Circuit

---

<sup>236</sup> *Mann*, 592 F.3d at 784.

<sup>237</sup> *See id.*

<sup>238</sup> *Id.* at 785.

<sup>239</sup> *Id.* (citing *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1013 (9th Cir. 2009) (Callahan, J., concurring in part and dissenting in part)).

<sup>240</sup> *Id.*

<sup>241</sup> *Id.* (citing *Comprehensive Drug Testing*, 579 F.3d at 1013 (Callahan, J., concurring in part and dissenting in part)).

<sup>242</sup> *See id.*

<sup>243</sup> *Id.* at 786.

<sup>244</sup> *Id.* at 785–86.

<sup>245</sup> *See id.* at 786.

reversed the district court's ruling with respect to the four images flagged by the KFF Alert, holding them inadmissible.<sup>246</sup> The court reasoned that the detective knew or should have known that any file tagged by the KFF Alert was likely child pornography, which was material outside the scope of the warrant.<sup>247</sup> By opening the files, the detective exceeded the scope of the original warrant that only authorized a "search for images of women in locker rooms or other private areas."<sup>248</sup> Besides these four images, the court held that the detective's actions "were reasonable and within the scope of the warrant's authorization."<sup>249</sup>

The Seventh Circuit reached the correct conclusion in *Mann* because it adhered to the principles of Fourth Amendment search and seizure doctrine. It ultimately rested its conclusion on whether the search was reasonable. The warrant authorized the officer to search for evidence of voyeurism, which meant he could open image files. In turn, any image he opened that turned out to be child pornography fell within the plain view doctrine. But the Seventh Circuit correctly distinguished the images tagged with a KFF Alert by reasoning that the officer should have known those images were likely child pornography. The facts of *Mann* were relatively straightforward; however, many different factual scenarios have come before other courts, and understanding these distinctions is important to fully grasp Fourth Amendment doctrine in the digital age.

#### IV. THE REASONABLE APPROACH: COMMON FACT PATTERNS TO GUIDE FUTURE COURTS

Besides the Seventh Circuit, the majority of other federal circuit courts that have addressed this issue continue to apply

---

<sup>246</sup> *Id.*

<sup>247</sup> *Id.* at 784.

<sup>248</sup> *Id.* at 781.

<sup>249</sup> *Id.* at 786 (citing *United States v. Grimmett*, 439 F.3d 1263, 1270 (10th Cir. 2006) (a computer search may be "as extensive as reasonably required to locate the items described in the warrant" (quoting *United States v. Wuagneux*, 683 F.2d 1343, 1352 (11th Cir. 1982)))).

traditional Fourth Amendment principles: a reasonableness standard, the particularity requirement, and the plain view doctrine.<sup>250</sup> Today's Fourth Amendment doctrine is the result of decades of continuously evolving court precedent. Digital evidence and computers should not cast doubt on this well-developed legal doctrine. Instead, it should be viewed as a continuation of the evolving common law.

As more digital evidence cases come before courts, the contours of the Fourth Amendment and digital evidence will become more apparent. Several common fact patterns have emerged, not all of which were implicated in *United States v. Mann*,<sup>251</sup> *United States v. Comprehensive Drug Testing, Inc.*,<sup>252</sup> or *United States v. Carey*.<sup>253</sup> These patterns will now be categorized and examined in order to provide a usable framework for future courts.

### A. *The Particularity Requirement*

The Fourth Amendment prohibits general warrants that authorize “exploratory rummaging in a person’s belongings.”<sup>254</sup> Instead, the Constitution requires that a warrant “particularly describ[e] the place to be searched, and the persons or things to be seized.”<sup>255</sup> Referred to as the particularity requirement, a warrant must “identif[y] the items to be seized by their relation to designated crimes” and must “leave[] nothing to the discretion of the officer executing the warrant.”<sup>256</sup>

---

<sup>250</sup> See *United States v. Williams*, 592 F.3d 511, 514 (4th Cir. 2010); *Mann*, 592 F.3d at 782; *United States v. Miranda*, 325 Fed. Appx. 858, 860 (11th Cir. 2009); *United States v. Carey*, 172 F.3d 1268, 1271 (10th Cir. 1999); *United States v. Turner*, 169 F.3d 84, 88–89 (1st Cir. 1999); *United States v. Henson*, 848 F.2d 1374, 1382 (6th Cir. 1988); *United States v. Gray*, 78 F. Supp. 2d 524, 528 (E.D. Va. 1999).

<sup>251</sup> See 592 F.3d at 780–82.

<sup>252</sup> See 579 F.3d 989, 993–94 (9th Cir. 2009).

<sup>253</sup> See 172 F.3d 1268, 1270–71 (10th Cir. 1999).

<sup>254</sup> *Andresen v. Maryland*, 427 U.S. 463, 480 (1976).

<sup>255</sup> U.S. CONST. amend. IV.

<sup>256</sup> *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010) (citing *Andresen*, 427 U.S. at 480–82).

Due to the vast amount of information that can be stored on a computer, the particularity requirement is becoming increasingly important in digital evidence cases.<sup>257</sup> Therefore, “warrants for computer searches must *affirmatively limit* the search to evidence of specific federal crimes or specific types of material.”<sup>258</sup> In other words, a warrant cannot authorize a search of an individual’s entire computer, where a police officer can “search from one object to another until something incriminating at last emerges.”<sup>259</sup> Nevertheless, the degree of specificity required is flexible, depends on the individual circumstances of each case, and “will vary depending on the crime involved and the types of items sought.”<sup>260</sup> Limiting the search to certain file types or crimes is important, but the warrant cannot be required to be so specific as to be a “constitutional strait jacket” on the executing officer.<sup>261</sup>

Magistrates are frequently confronted with a situation where prior to the actual search, the officers do not know exactly what type of computer devices an individual has in his possession.<sup>262</sup> As a result, warrants often broadly describe the type of physical devices to be searched and seized.<sup>263</sup> In order for the warrant to meet the particularity requirement, the generality regarding the physical units to be seized needs to be counterbalanced with limitations on the specific content to be searched for within the computer.<sup>264</sup>

---

<sup>257</sup> See *United States v. Riccardi*, 405 F.3d 852, 862 (10th Cir. 2005).

<sup>258</sup> *Id.* (emphasis added).

<sup>259</sup> *Coolidge v. New Hampshire*, 403 U.S. 443, 466 (1971).

<sup>260</sup> *United States v. Henson*, 848 F.2d 1374, 1383 (6th Cir. 1988); see also *United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997) (holding that the generic classification in the language of the warrant was acceptable since “no more specific description of the computer equipment sought was possible”).

<sup>261</sup> *United States v. Phillips*, 588 F.3d 218, 223 (4th Cir. 2009).

<sup>262</sup> *E.g.*, *United States v. Williams*, 592 F.3d 511, 520–21 (4th Cir. 2010); *Henson*, 848 F.2d at 1382–83.

<sup>263</sup> See generally *United States v. Mann*, 592 F.3d 779, 780–81 (7th Cir. 2010) (warrant authorizing search for “video tapes, CD’s or other digital media, computers, and the contents of said computers, tapes, or other electronic media”); *United States v. Burgess*, 576 F.3d 1078, 1083 (10th Cir. 2009) (authorizing a search of “computer records”).

<sup>264</sup> See *United States v. Riccardi*, 405 F.3d 852, 862 (10th Cir. 2005).

An illustration of a warrant meeting the particularity requirement in the digital context is the Ninth Circuit's *United States v. Burgess*.<sup>265</sup> The warrant in *Burgess* authorized a search for "computer records" that "would tend to show conspiracy to sell drugs, including pay-owe sheets, address books, rolodexes, pagers, firearms and monies."<sup>266</sup> The Ninth Circuit held that the warrant was not overly broad since it "contained sufficiently particularized language' creating 'a nexus' with the crime to be investigated."<sup>267</sup>

In contrast, *United States v. Otero* provides an example of an overly broad warrant that did not meet the particularity requirement.<sup>268</sup> The police suspected that Otero, a postal worker, was stealing letters from credit card companies that were supposed to be delivered on his route.<sup>269</sup> After planting two test letters that failed to be delivered, the police executed a warrant to search Otero's house.<sup>270</sup> The warrant authorized a search for "any and all information and/or data stored . . . on computer media . . ."<sup>271</sup> The warrant did not limit the search to certain computer file types (i.e., Word documents, PDF files, or image files), nor did it limit the specific content to be searched (i.e., evidence of mail or credit card fraud).<sup>272</sup> The Tenth Circuit held that the warrant failed to describe the items to be seized with "technical precision [or] practical accuracy, and it therefore lack[ed] sufficient particularity."<sup>273</sup>

---

<sup>265</sup> 576 F.3d at 1091

<sup>266</sup> *Id.* at 1083.

<sup>267</sup> *Id.* at 1091 (citing in part *United States v. Grimmett*, 439 F.3d 1263, 1271 (10th Cir. 2006); see also *Mann*, 592 F.3d 780–81 (warrant authorizing a search of computers only for "images of women in locker rooms or other private areas"); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999).

<sup>268</sup> 563 F.3d 1127, 1133 (10th Cir. 2009).

<sup>269</sup> *Id.* at 1129.

<sup>270</sup> *Id.*

<sup>271</sup> *Id.* at 1130.

<sup>272</sup> See *id.*

<sup>273</sup> *Id.* at 1132; see also *United States v. Riccardi*, 405 F.3d 852, 863 (10th Cir. 2005) (holding that a search was invalid because it did not limit the search to any particular files or any particular federal crime. "The warrant thus permitted the officers to search for anything—from child pornography to tax returns to private correspondence.").

A warrant must be as specific as the circumstances allow.<sup>274</sup> If a warrant authorizes the seizure of any computer device and search for any incriminating evidence, a court will likely hold any file found pursuant to the warrant to be inadmissible.<sup>275</sup> Instead, a warrant must affirmatively state either (1) the type of documents to be searched for (documents, images, videos, etc.) or (2) the type of content to be searched for (financial data, pornographic images, drug activity, etc.).<sup>276</sup> The more specific a warrant, the more likely computer files seized pursuant to that warrant will be held admissible in court.

### *B. Common Fact Patterns under the Plain View Doctrine*

There are many factual scenarios that may arise when an officer is searching a computer. These factual complexities make it difficult to craft a clear, black-and-white rule for digital evidence cases. Below are summaries of common factual scenarios and illustrations of how courts have determined whether digital evidence fell within the plain view doctrine. By understanding how the plain view doctrine has been applied so far, future courts will be able to better understand how to decide new and complex issues that will arise in future digital evidence cases.

#### 1. Was the officer looking for the same types of files listed in the warrant?

To meet the particularity requirement, a warrant must affirmatively state either the type of files or specific content to be searched for.<sup>277</sup> In practice, it is very difficult for an officer to tightly restrict his search but still conduct a thorough investigation.<sup>278</sup> As several courts readily point out, it is very unlikely for a criminal to

---

<sup>274</sup> *United States v. Henson*, 848 F.2d 1374, 1383 (6th Cir. 1988).

<sup>275</sup> *See Otero*, 563 F.3d at 1132.

<sup>276</sup> *See Riccardi*, 405 F.3d at 862.

<sup>277</sup> *Id.*

<sup>278</sup> *See generally Henson*, 848 F.2d at 1383.

label or organize computer files so their criminality is readily apparent.<sup>279</sup>

There are a number of ways to manipulate computer files to disguise their illegal nature. The easiest way is to use a deceptive file name.<sup>280</sup> Few criminals “keep documents of their criminal transactions in a folder marked ‘criminal records.’”<sup>281</sup> If an individual has a Word document with the recipe for manufacturing methamphetamine, he can disguise this file’s true nature by naming it anything other than “meth stuff.”<sup>282</sup> File names for images can be even more deceptive. Computers will often automatically name an image file with a seemingly random file name—for example, “Img\_5777\_875.jpg” or “DC001352.jpg.”<sup>283</sup> These types of file names give no indication of the file’s content, so an officer must open each file in order to see what the file actually contains.<sup>284</sup>

A second way to hide incriminating evidence is to change the file extension type. There are dozens of different file types.<sup>285</sup> By modifying a file’s extension, an individual can conceal the true file type and even prevent the file from being opened.<sup>286</sup> For example, if a file was created as a Microsoft Word document (.doc) and is subsequently changed to an Adobe file (.pdf), the file will be unreadable and cannot be opened.<sup>287</sup> Some software programs used by

---

<sup>279</sup> See *United States v. Hill*, 459 F.3d 966, 978 (9th Cir. 1999) (“Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer.”); *United States v. Gray*, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999) (holding a criminal will “often intentionally mislabel files, or attempt to bury incriminating files within innocuously named directories”).

<sup>280</sup> See *Gray*, 78 F. Supp. 2d at 528.

<sup>281</sup> *Id.*

<sup>282</sup> See *United States v. Burgess*, 576 F.3d 1078, 1093 (10th Cir. 2009).

<sup>283</sup> See *id.* at 1093–94.

<sup>284</sup> See *id.*

<sup>285</sup> See *id.* at 1093 (e.g., .txt, .doc, .docx, and .dot for Microsoft Word; .wpt, .wpk, and .wpd for WordPerfect; .pdf for Adobe; .xls, .xlsx, and .xltx for Microsoft Excel; or .jpg and .gif for images).

<sup>286</sup> *Kerr*, *supra* note 128, at 545.

<sup>287</sup> See *id.*

police can detect these unreadable files and determine the correct file extension. The lesson, however, is the same: officers cannot limit their searches to certain file types.<sup>288</sup>

The third common way to conceal incriminating documents is to hide incriminating files among innocuous files.<sup>289</sup> By burying incriminating files among dozens or even hundreds of unrelated, noncriminal files, law enforcement has much more difficulty locating the types of files authorized for search and seizure by the warrant.<sup>290</sup>

Although a warrant must state the types of files or content to be searched for, “[i]t is unrealistic to expect a warrant to prospectively restrict the scope of a search by [a specific] directory, filename or extension.”<sup>291</sup> This does not mean that officers can look at every single file on a computer. Instead, the officer should “look in the most obvious places . . . But in the end, there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders.”<sup>292</sup>

In sum, it is unrealistic to expect a magistrate to be able to prospectively limit a search to certain file types or names since law enforcement personnel rarely know what information they are going to find on a computer. When an officer begins his search, he should look in the most obvious places—either by using a keyword search or manually searching the computer for files whose names indicate that they are within the scope of the warrant. If this initial inquiry uncovers nothing, then the officer can broaden his search by cursorily looking at all files on the computer to determine whether the content is relevant and within the scope of the warrant.

---

<sup>288</sup> *See id.*

<sup>289</sup> *United States v. Gray*, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999) (“[C]omputer hackers often intentionally mislabel files, or attempt to bury incriminating files within innocuously named directories.”).

<sup>290</sup> *See id.*

<sup>291</sup> *United States v. Burgess*, 576 F.3d 1078, 1093 (10th Cir. 2009).

<sup>292</sup> *Id.* at 1094.

## 2. Did the officer open the files cursorily?

Since the content of computer files can be so easily disguised, an officer executing a warrant must often open each file to determine whether its falls within the scope of the warrant.<sup>293</sup> Some defendants have argued that this essentially turns every computer search into a general search.<sup>294</sup> However, having to cursorily open computer files can be equated with traditional physical evidence seizures, where cursorily examining files is acceptable.

The Supreme Court has held that when searching through large files of business documents, “it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.”<sup>295</sup> For example, the Fourth Circuit held that officers acted lawfully when they briefly read a letter found in the defendant’s apartment that detailed a recipe for making methamphetamine.<sup>296</sup> Since the letters were within plain view, the court held that “some perusal, generally fairly brief, of the documents was clearly necessary in order for the police to perceive the relevance of the document to crime.”<sup>297</sup> After briefly reading the documents, their incriminating nature became immediately apparent and subject to seizure under the plain view doctrine.<sup>298</sup>

Just like searching through physical documents, an officer searching through hundreds or thousands of computer files must cursorily open each document to determine its content.<sup>299</sup> If the file’s criminality becomes immediately apparent after opening it, then the file may be lawfully seized under the plain view doctrine.<sup>300</sup> For example, in *United States v. Gray*, the Northern District of Virginia

---

<sup>293</sup> See *United States v. Williams*, 592 F.3d 511, 521–22 (4th Cir. 2010)

<sup>294</sup> See, e.g., *United States v. Mann*, 592 F.3d 779, 782 (7th Cir. 2010); *United States v. Carey*, 172 F.3d 1268, 1271–72 (10th Cir. 1999).

<sup>295</sup> *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976).

<sup>296</sup> *United States v. Crouch*, 648 F.2d 932, 933 (4th Cir. 1981).

<sup>297</sup> *Id.* (quoting *United States v. Ochs*, 595 F.2d 1247, 1257 n.8 (2d Cir. 1979)).

<sup>298</sup> *Id.* at 934.

<sup>299</sup> See *United States v. Williams*, 592 F.3d 511, 521–22 (4th Cir. 2010).

<sup>300</sup> See *id.* at 522.

held that an officer could open computer records to determine the computer's content.<sup>301</sup> An FBI agent was executing a search for evidence of unauthorized government computer intrusions.<sup>302</sup> He utilized a software program that created a directory of the computer files, and he followed FBI protocol by opening and looking "briefly at each of the files contained in the directories."<sup>303</sup> The agent discovered child pornography in a folder titled "Tiny Teen."<sup>304</sup> The court, however, held that his search of the folder was a lawful continuation of his original search.<sup>305</sup> The FBI agent testified that he "knew from his experience that computer hackers often intentionally mislabel files, or attempt to bury incriminating files within innocuously named directories."<sup>306</sup> It was improper to limit computer searches to certain file names because "the designation or labeling of files on a computer can easily be manipulated to hide their substance."<sup>307</sup>

This position is supported by practical considerations. If police could examine only files with certain names or file types, criminals would have an obvious advantage over law enforcement. This standard would induce every criminal, knowing that the police's hands are so tightly tied behind their backs, to label incriminating computer files with innocuous names and bury the files among innocent content. This would be a perverse result because it would make law enforcement efforts more difficult and would reduce the likelihood that someone will be arrested for illegal activity.

An analogy of this impracticable standard to physical evidence would be a rule that precluded police from seizing a bag containing a powdery white substance if it is labeled "flour" or "talcum powder."<sup>308</sup> In order to determine the contents, the powdery substance must be tested.<sup>309</sup> Similarly, a computer file must be cursorily examined in

---

<sup>301</sup> *United States v. Gray*, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999).

<sup>302</sup> *Id.* at 526.

<sup>303</sup> *Id.*

<sup>304</sup> *Id.* at 527.

<sup>305</sup> *Id.* at 530.

<sup>306</sup> *Id.* at 529.

<sup>307</sup> *United States v. Williams*, 592 F.3d 511, 522 (4th Cir. 2010).

<sup>308</sup> Ziff, *supra* note 64, at 864.

<sup>309</sup> *Id.*

order to determine its content. The principles relating to physical searches should be extended to digital searches in order to allow police to conduct a thorough and effective computer search.

3. After uncovering material outside the scope of the warrant, did the officer stop his search and get a second warrant for the newly discovered evidence?

Although officers can cursorily open documents on a computer, what the officer does after discovering incriminating files outside the scope of the warrant becomes important. Some courts have held that the officer must stop his search and obtain a second warrant for the newly discovered incriminating evidence.<sup>310</sup> Indeed, this is the most prudent course of action an officer can take when he uncovers evidence outside the scope of the warrant.

For example, in *United States v. Burgess*, when the officer discovered child pornography that was outside the scope of the warrant, he immediately stopped his search and obtained a second warrant to search for the child pornography.<sup>311</sup> The Tenth Circuit held that the first image the officer viewed was admissible under the plain view doctrine.<sup>312</sup> But the officer did not exceed the scope of the warrant because he immediately stopped his search and did not renew it until he received a second warrant.<sup>313</sup> The first image established probable cause for the second warrant, and the images later discovered under the second warrant were admissible.<sup>314</sup> The court did note that had the first image had a filename “strongly suggesting pornography,” the officer could not have legally opened the file since he would have had reason to know that its content was outside the scope of the

---

<sup>310</sup> See *United States v. Burgess*, 576 F.3d 1078, 1092 (10th Cir. 2009); *Gray*, 78 F. Supp. at 527–28 (E.D. Va. 1999).

<sup>311</sup> 576 F.3d at 1092; see also *Gray*, 78 F. Supp. 2d at 527–28 (holding that child pornography was admissible because the officer obtained a second warrant after inadvertently discovering child pornography).

<sup>312</sup> See *Burgess*, 576 F.3d at 1092.

<sup>313</sup> *Id.* at 1094–95.

<sup>314</sup> See *id.* at 1084, 1094–95.

warrant.<sup>315</sup> The officer would have had probable cause, but would have had to secure a second warrant before proceeding.<sup>316</sup>

4. If clear, what were the subjective intentions of the officer?

Courts should consider the subjective intent of the officer when their intent is clear. For example, the detective in *United States v. Carey* admitted to stopping his original search and beginning a second search for child pornography.<sup>317</sup> The subjective intent of the officer clearly indicated that his search was outside the scope of the warrant.<sup>318</sup>

However, a subjective intent analysis should be restricted to situations where the intent of the officer is clear and he admits to starting a second, unauthorized search. As discussed previously, there is an incentive for police officers to testify that their search did not go beyond the scope of the warrant.<sup>319</sup> However, if an officer admits in court that he intended to go beyond the scope of the warrant, that evidence is relevant in determining whether the seized evidence should be suppressed.

## CONCLUSION

The traditional principles of Fourth Amendment search and seizure doctrine—reasonableness, the particularity requirement, and the plain view doctrine—should continue to be the standard that courts apply in both physical and digital evidence cases. Established in a pre-computer era, these principles should be allowed to gradually evolve into the realm of digital evidence. Both the Ninth and Tenth Circuits

---

<sup>315</sup> *Id.* at 1095.

<sup>316</sup> *Id.*

<sup>317</sup> 172 F.3d 1268, 1273 (10th Cir. 1999); *see also* *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1010 (9th Cir. 2009) (holding that the federal agent exceeded the scope of the warrant because he intentionally “peruse[d the file] to see if there was anything above and beyond that which was authorized for seizure in the initial warrant”).

<sup>318</sup> *See Carey*, 172 F.3d at 1273.

<sup>319</sup> *See id.* at 1271.

have departed from this sound precedent prematurely and have crafted alternative approaches that either go against Supreme Court precedent or create as many problems as they solve. The Seventh Circuit, in *United States v. Mann*, reached the correct conclusion and properly applied court precedent. The prevalence of computers in American society and the higher potential for privacy invasions is a concern of which courts should take note. However, the prudent and correct approach for future courts is to abide by settled court precedent and expand the doctrines incrementally as needed.