**NO. 18-5578**

---

**UNITED STATES COURT OF APPEALS**
**FOR THE SIXTH CIRCUIT**

---

**UNITED STATES OF AMERICA**

**Plaintiff-Appellee,**

**v.**

**WILLIAM J. MILLER,**

**Defendant-Appellant.**

---

**On Appeal From The Judgment**
**Of The United States District Court**
**For the Eastern District of Kentucky at Covington**
**Honorable David L. Bunning**

---

**District Court No. 2:16-cr-00047-1**

---

# REPLY BRIEF OF APPELLANT WILLIAM J. MILLER

---

ERIC G. ECKES
(CJA Appointed)
Pinales Stachler Young Burrell & Crouse Co., L.P.A.
455 Delta Ave., Suite 105
Cincinnati, Ohio 45226
Telephone: (513) 252-2723
Fax: (513) 252-2751

**ORAL ARGUMENT REQUESTED**

# TABLE OF CONTENTS

# TABLE OF AUTHORITIES

## Federal Cases

**Journals**

## REPLY TO APPELLEE'S BRIEF

### I. The District Court Erred when Denying Miller's Motion to Suppress.

All parties agree Miller's suppression issue is novel and a matter of first impression for this Circuit. Recently, the Fifth Circuit has weighed in on the issue in a case with facts similar to the instant case. *See United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018). In the United States' response, as one would expect, heavy reliance is placed on the Fifth Circuit's analysis. Counsel is aware that cases with similar facts and issues are arising throughout the country in state and federal courts. As described below, Miller respectfully requests this Court not reach the same result as the Fifth Circuit for multiple reasons.

Critically, the Fifth Circuit does not address the traditional trespass inquiry. In the words of the Fifth Circuit, "[t]he private search doctrine decides this case." *Id*. at 637. While Miller disagrees with the Fifth Circuit's application and unwarranted expansion of the private search doctrine, and urges this Court to not follow suit, the analysis does not begin and end with a doctrine that only applies as an exception to the warrant requirement for the *Katz* test. As stated by the Supreme Court, "Fourth Amendment rights do not rise or fall with the *Katz* formulation." *United States v. Jones*, 565 U.S. 400, 406 (2012).

One of the foundational arguments asserted in Miller's opening brief was that the traditional trespass inquiry is not limited by the private search doctrine. To that end, the private search doctrine alone does not decide this case. Citing *Carpenter v. United States*, Miller argued in his opening brief that simply because a private party uses a modern technology to invade a person's reasonable expectation of privacy in their email attachments, the "Fourth Amendment protections for your paper and effects do not automatically disappear." 138 S.Ct. 2206, 2268 (Gorsuch, N. dissenting). Pursuant to the original understanding of the Fourth Amendment, where the framers never would have dreamed of the modern technology at play in this case, "the traditional approach asked if a house, paper, or effect was *yours* under law. No more was needed to trigger the Fourth Amendment." *Id*. at 2267-68 (emphasis in the original).

In response, the United States mostly ignores Miller's argument involving the straightforward application of the traditional approach to the facts of this case.[1] Tellingly, the United States effectively concedes that an email attachment would qualify as a constitutionally protected space (a paper or effect), but then suggests

[1] Notably, the Amici Curiae tech companies supporting the United States failed to address, or even acknowledge, the traditional trespass inquiry presented in Miller's opening brief.

that Detective Schihl's invasion of that space was not a "physical intrusion." (Response, R. 34, Page ID# 28).

Notwithstanding the confusion engendered by the United States' semantics about what is a "space" and the physics of occupying it, the government's argument is not consistent with the original understanding of the Fourth Amendment. As stated by then Judge Gorsuch for the Tenth Circuit, the "warrantless opening of (presumptively) private correspondence . . . seems *pretty clearly to qualify as exactly* the type of trespass to chattels [*i.e.* physical intrusion] the framers sought to prevent when adopting the Fourth Amendment." *United States v. Ackerman*, 831 F.3d 1292, 1308 (10th Cir. 2016) (emphasis added). Judge Gorsuch further explained, "no one in this appeal disputes that email is a 'paper' or 'effect' for Fourth Amendment purposes, a form of communication capable of storing all sorts of private and personal details, from correspondence to images, video, or audio files, and so much more." *Id*. at 1304.

An email attachment is a package. *See Reddick*, 900 F.3d at 639 (referring to computer files as "packages"). The Sixth Circuit has recognized that distinct and different files operate as distinct and separate containers or packages. *United States v. Lichthenberger*, 786 F.3d 478 (6th Cir. 2015) (adopting a "file" as a distinct unit of measurement for analyzing Fourth Amendment issue in the context of the

private search doctrine). In effect, the entire process of sending an email and its attachments is a modern way to send correspondence—a modern way to send a "package" or container through the mail. Thus, just like correspondence from the time of the adoption of the Fourth Amendment, the package must be opened (or trespassed upon) to view the contents. This is exactly what Detective Schihl did when he opened the email attachments. He opened a package; his actions in doing so need not be complicated. A new definition of the word "space" is not needed. Opening a package (in this case a file) is a physical intrusion, just as it was when law enforcement opened an envelope of mailed correspondence at the time of the Fourth Amendment's adoption.

For a well-reasoned—albeit complicated—explanation of the technical foundation for how opening a file is a trespass to chattels, see "You've Got Mail!" Decoding the Bits and Bytes of Fourth Amendment Computer Searches After Ackerman." 94 Denv. L. Rev. 651 (2017). In short, "the 'chattel' that is trespassed is the data," or the contents inside the file. *Id*. at 677. Furthermore,

> A file is directly analogous to real property because the file structure itself represents the 'fence' of the property, and the data contained within the file represents the land and other possessions contained within the fence. The conceptual framework is simple: opening a file is akin to crossing the fence or real property.

*Id*. at 678.

In addition to the traditional trespass analysis, Miller continues to argue that Detective Schihl's search of the email attachments exceeded the original Google search of Miller's email account. The government's response relies entirely on the private search doctrine. However, the private search doctrine does not operate to excuse a warrantless search when the government performs a different type of search than that performed by the private party, particularly when the purpose of the additional search is to learn the actual (not theoretical) contents of a package, which would later be used for trial. Here, Detective Schihl performed a different type of search than the Google search, and his purpose was to collect the contents of the package so that he could use the actual contents as evidence at trial.

Because Detective Schihl opened a previously unopened package to obtain evidence for trial, the proper analogue is *Walter v. United States*, 447 U.S. 649, 654 (1980). As determined in *Walter*, an unconstitutional search takes place when the government conducts "[f]urther investigation – that is to say, a search of the contents" of a package when that additional search/investigation ". . .was necessary in order to obtain the evidence which was to be used at trial." *Id.* The United States' evidence at trial was not hash values. The evidence presented at trial was the contents of the specific package as discovered by Detective Schihl.

Ultimately, Detective Schihl's search aligns with striking similarity to the

following description in *Walter*:

> Even though the cases before us involve no invasion of the privacy of the home, and notwithstanding that the nature of the contents of these films [*i.e.* email attachments] was indicated by descriptive material on their individual containers [*i.e.* hash values], we are nevertheless persuaded that the unauthorized exhibition of the films [*i.e*. opening of the email attachment] constituted an unreasonable invasion of their owner's constitutionally protected interest in privacy. It was a search; there was no warrant; the owner had not consented; and there were no exigent circumstances.
>
> It is perfectly obvious that the agents' reason for viewing the films [*i.e*. opening the email attachments] was to determine whether their owner was guilty of a federal offense. To be sure, the labels on the film boxes [*i.e.* hash values] gave them probable cause to believe that the films were obscene [*i.e* contained child pornography] and that their shipment in interstate commerce had offended the federal criminal code. But the labels [hash values] were not sufficient to support a conviction . . . Further investigation -- that is to say, a search of the contents of the films [email attachments] -- was necessary in order to obtain the evidence which was to be used at trial.
>
> The fact that FBI agents were lawfully in possession of the boxes of film did not give them authority to search their contents. Ever since 1878 when Mr. Justice Field's opinion for the Court in *Ex parte Jackson*, 96 U.S. 727, established that sealed packages in the mail cannot be opened without a warrant, it has been settled that an officer's authority to possess a package is distinct from his authority to examine its contents.

*Walter*, 447 U.S. at 654.

The United States' reliance on *Jacobsen* is misplaced. In *Jacobsen*, the mail carrier opened a damaged package to examine its contents for private, non-governmental purposes. 466 U.S. 109, 111 (1984). Inside, the carrier discovered a

white powder that appeared to be cocaine. *Id.* The DEA was subsequently notified. *Id.* When DEA agents arrived, the box had a hole punched in the side and the top open. *Id.* The agent then re-examined the package, removed the cocaine, and performed a field test to confirm the identity of the substance. *Id.*

When the agent in *Jacobsen* re-examined the package to find suspicious white powder, the search was the same type of search conducted by the private party. In other words, he re-examined the same package that was unsealed by the private party, and thus, it was the private party that frustrated the reasonable expectation of privacy in that specific package (the box). In Miller's case, the package is the email attachment. As argued, it was not previously opened. It was a sealed package, and the resulting intrusion upon it was not a re-examination, but rather the first examination of that specific package.

In addition, when discussing the drug testing of the cocaine, the Fifth Circuit's analysis problematically conflated two separate issues in *Jacobsen*, which included: 1) the search of the box to find its contents (the cocaine), and 2) the drug testing of the cocaine. When the issues are separated out, it becomes clear that opening the email attachment is not akin to the drug testing of the cocaine.

As stated, the email attachment was a package. People have reasonable expectations of privacy in packages. The cocaine was cocaine; it was not a package

that the police opened. It was the *actual contents* inside of the package. Thus, drug testing the contents of the package, which appeared to be contraband, was not a search because no private fact about cocaine is learned by drug testing it. *Jacobsen*, 466 U.S. at 123. In contrast, opening an email attachment is the same as opening a package, and such action is a search because packages may contain compromising and private information inside of them. Perhaps, running some sort of testing on the contents (*i.e.* the data) inside the email attachment file would be akin to drug testing the cocaine, but that is not the issue here. In the end, the cocaine drug test analysis in *Jacobsen* is a red herring when applied to the facts of the instant case.

Furthermore, the "virtual certainty" language from *Jacobsen* injects confusion into an otherwise simple issue. The "virtual certainty" test should be applied when law enforcement *re-examines* "persons, houses, papers, and effects" that have already been opened through a prior private search. *See Jacobsen*, 466 U.S. at 118-19. But there was no prior search in Miller's case; the virtual packages were unopened. In other words, the seal remained intact on the virtual packages.[2] In this regard, the "virtual certainty" analysis is inapplicable because such an

[2] In *Jacobsen*, the package being re-examined "had previously been opened, [and] remained unsealed," which was "highly relevant to the reasonableness of the agent's conduct . . ." *Jacobsen*, 466 U.S. 109, 121.

analysis only need be conducted when law enforcement searches a previously searched container like the box in *Jacobsen*.

In short, Detective Schihl's conduct was a physical trespass on Miller's constitutionally protected space, thereby triggering Fourth Amendment protection. As discussed above, the traditional trespass inquiry is not limited by the private search doctrine exception to *Katz*. Alternatively, Miller's reasonable expectation of privacy in his email attachments was violated when Detective Schihl exceeded the scope of the prior search by Google. Finally, as detailed in Miller's opening brief, Google should be declared a state actor for its nexus relationship with NCMEC, which is a state actor serving a governmental function. As such, Miller's convictions should be reversed, and his case remanded for a new trial.

## II. Miller's Due Process Rights and his Right to Confrontation, Pursuant to the Fifth and Sixth Amendments of the United States Constitution, Were Violated when the District Court Overruled his Objection to the Admission of the Cybertipline Report.

The record reveals that counsel made numerous objections to the admission of the CyberTipline Report based on the work of a non-testifying analyst. Prior to the report's admission, counsel objected to the executive director of NCMEC's Exploited Children Division's lack of personal knowledge, stating ". . . the investigation that happens by people that are not this witness – the executive director doesn't get online and investigate. . . . She doesn't know what the analyst

did. She doesn't have that personal knowledge." (Jury Trial Day 1 Tr., R. 95, Page ID # 533). Counsel continued, "She can testify to what an analyst does. She can't testify to what this analyst did." (*Id.*). In short, while counsel objected to the hearsay of the report in general, he also objected to the executive director testifying about a non-testifying analyst's statements. This objection was later supplemented with precise language from Confrontation Clause jurisprudence. (*Id.* at Page ID # 550-51) ("Just on the prior objection, I just want to raise the case law of *Crawford* in addition to it, because it's – I've articulated this, but I didn't use the word *Crawford*."). Therefore, the proper standard of review is *de novo*. *United States v. Warman*, 578 F.3d 320, 345 (6th Cir. 2009) ("Generally, we review the district court's evidentiary rulings for abuse of discretion, but challenges made under the Confrontation Clause are reviewed *de novo*.").

The Government's argument confuses matters by classifying the issue as an evidentiary issue under Rule 803(6). Here, the issue is not solely concerned with admitting the report as a business record because business records are not immune from scrutiny under the Confrontation Clause. *Melendez-Diaz v. Massachusetts*, 557 U.S. 305 (2009). Rather, the Court must determine whether the NCMEC analyst should be subject to confrontation under the Sixth Amendment.

Contrary to the Government's assertion, NCMEC's process for resolving the IP addresses to a specific location is entirely unclear from the record. During trial, the executive director of NCMEC's Exploited Children Division gave conflicting statements regarding the analysts' involvement in the process. Initially, the executive director stated, "So the reports come in, and the analysts may add additional value to the report. They may review the information that's been provided and *try to locate or provide a location*." (Jury Trial Day 1 Tr., R. 95, Page ID # 529) (emphasis added). The executive director later testified that Section B of the Cyber Tipline report, the section listing the location of the IP addresses, contains automated information. (*Id.* at Page ID#541-42). This distinction is especially important when an analyst's compilation, transcription, manipulation, or interpretation of machine-generate data all fall within the purview of the Confrontation Clause. *See United States v. Lamons*, 532 F.3d 1251 (11th Cir. 2008).

The key to this issue involves the overall inability for Miller to confront the evidence used against him. Indeed, an erroneous admission of the Cybertipline Report became drastically compounded during the United States' rebuttal argument. In this way, the Confrontation Clause violation continued into the government's closing argument, gaining traction with an additional egregious

violation of due process, which occurred when the government mischaracterized the Cybertipline Report and added inaccurate facts not in evidence.

Indeed, statements made by the Government during rebuttal amounted to misconduct in violation of the Due Process Clause and the Confrontation Clause. The Government's statement about the IP addresses resolving back to Miller's house placed before the jury facts not in evidence *and not subject to confrontation*. Since the Government was not a witness, its statement could not be tested by cross-examination. Nor was Miller afforded *any opportunity* to redress the denial of his right secured by the Confrontation Clause because the statement was admitted during the Government's rebuttal closing argument. A violation of the Confrontation Clause is not a harmless error unless the reviewing court finds it was harmless beyond a reasonable doubt. *Bulls v. Jones*, 274 F.3d 329, 334-35 (6th Cir. 2001).

Miller was forced to sit back as the jury deliberated with the realization that his entire defense had been obliterated with an incriminating mischaracterization of the inadmissible evidence in the Cybertipline Report. The situation went from Miller being unable to cross the analyst to being unable to cross the government's misstatement about the work of the analyst. In this way, the original confrontation clause violation was exacerbated, and this was error. In addition, the statement in

rebuttal by the government itself was error and a violation of the Confrontation Clause and Due Process Clause.

Given the context of the Government's statement, it injected significant prejudice into the proceedings. It is well-settled that the Government may not rely on facts not in evidence in closing arguments. *United States v. Wiedyk*, 71 F.3d 602, 610 (6th Cir. 1995) ("A prosecutor's statement in a closing argument is improper if the statement brings to the jury's attention purported facts that are not in evidence and are prejudicial."). The Supreme Court has found that "some remarks included in . . . [a] closing statement could be so prejudicial that a finding of error, or even constitutional error, would be unavoidable." *Frazier v. Cupp*, 394 U.S. 731, 735-36 (1969).

A prosecutor's improper statement rises to the level of reversible error when it is flagrant. *Id.* To determine whether a statement is flagrant, the court must examine the following four factors: (1) "whether the remarks tended to mislead the jury or to prejudice the accused [including whether the trial judge gave an appropriate cautionary instruction to the jury]; (2) whether they were isolated or extensive; (3) whether they were deliberately or accidentally placed before the jury; and (4) the strength of the evidence against the accused." *United States v. Abboud*, 438 F.3d 554, 584 (6th Cir. 2006) (citation omitted). If the statement was

not flagrant, the court may still reverse if (1) "the proof against the defendant was not overwhelming, (2) opposing counsel objected to the conduct, and (3) the court failed to give a curative instruction." *Id.*

Importantly, the Government conceded in its response that the assertion regarding the IP addresses resolving to Miller's residence was improper. (Appellee's Brief, R. 34, Page 37). Furthermore, in balancing the above factors, the Government's statement was flagrant. The statement clearly bore on a fundamental part of the Government's case against Miller. In addition, the Government made deliberate argument regarding the improper statement:

> The other issue with the IP address is, ladies and gentlemen, I suggest you take a look at the Cyber Tipline report, because NCMEC geo resolved both of the IP addresses that were given to it. The IP address of the initial login, the created date of the Gmail account, and the IP address that was captured in the email on July 9th of 2015 that contained those two images of the – disabled his account, they both resolved back to Time Warner Cable at the exact same latitude and longitude. The defendant's house.

(Jury Trial Day 3 Tr., R. 97, Page ID # 891). Thereafter, the Government repeatedly referred to the fact that Miller's brother, the alternative suspect, would have needed to commit the alleged offenses at Miller's house. (*Id.* at Page ID#893) ("None of the information that they conveyed would lead anybody with even a modicum of common sense to believe that he was the one sitting at the defendant's home using his internet access, chatting hours upon hours each day with

individuals . . .”); (*Id.* at Page ID#895) (“He wants you to find that his mentally deficient brother, who comes to his house maybe two times a month, maybe two or three times a week, depending on who you believe, came to his house . . .”).

These statements placed the location of the IP addresses before the jury in a way that “may well have been equivalent in the jury’s mind of testimony,” *Douglas v. Alabama*, 380 U.S. 415, 419 (1965), and the statement “added substantial, perhaps even critical, weight to the Government’s case in a form not subject to cross-examination.” *Bruton v. United States*, 391 U.S. 123, 128 (1968). The CyberTipline Report was admitted as part of a batch of evidence aimed at proving that Miller had uploaded child pornography onto a specific Google account. Miller maintained the same defense throughout trial: Somebody else, presumably Fred Miller, was using the email address where the child pornography was distributed and received. To that end, it was critical to recognize that the Creation IP in January of 2015 was not Miller’s known public IP address. (Jury Trial Day 3 Tr., R. 95, Page ID # 877).

The only piece of evidence the Government could have relied on to establish the creation IP address was the CyberTipline Report. However, the Government incorrectly portrayed to the jury that the two separate IP addresses both resolved back to the same location: Miller’s house. Importantly, counsel objected to facts

not in evidence, but the objection was overruled. Thus, no curative instructions were given to the jury. Now that the government concedes the connection of the IP addresses to Miller's house was improper, this means that the correct fact (which could have been discussed in a cross of the analyst) is that the IP addresses *do not attach* to Miller's home—a fact that is exculpatory. Thus, the Government's misconduct placed before the jury facts not in evidence that significantly prejudiced Miller.

Whether viewed through the lens of a Confrontation Clause violation due to the admission of the Cybertipline report exacerbated by the rebuttal argument, or as a Confrontation Clause/Due Process violation based on the presentation of inaccurate facts not in evidence, the result is the same: Miller's convictions should be reversed, and his case remanded for a new trial.

## III. The District Court Erred when Denying Miller's Rule 29 Motion as there was Insufficient Evidence for All Counts.

The Government's argument incorrectly analogizes the issue presented in Miller's opening brief with the issue presented in *United States v. Lowe*, 795 F.3d 519 (6th Cir. 2015). While the shared access to the Acer laptop and Toshiba external hard drive are relevant to the possession count, the distribution and receipt counts implicate the shared access to the miller694u@gmail.com email account. In attempting to distinguish *Lowe*, however, the Government completely ignores the

ample evidence linking a second user to the miller694u@gmail.com email account. Miller's statements may be proper to consider as they relate to the possession count and the external hard drive, but his statements were clear that he did not send or receive child pornography.

As set forth in the opening brief, the evidence presented at trial established that someone other than Miller, namely Fred Miller, had shared access to both the email account and the external hard drive in question. Although the email account was subscribed to by "William Miller," this alone is insufficient to support Miller's convictions. *See Lowe*, 795 F.3d at 523 (holding that it was unreasonable to infer that the defendant had downloaded child pornography even though a nickname close to his real name was used when downloading software and visiting websites). This rings especially true when the miller694u@gmail.com email inbox contained multiple automated Google alerts stating there were new sign-ins from various possible locations—including a new sign-in alert on a date of distribution/receipt—and several emails addressed to "Fred" regarding the purchase of an LG cell phone and tablet. (*Id.* at Page ID # 669-70, 674-79).

Based on the foregoing, and the reasons detailed in the opening brief, the State failed to prove that Miller had exclusive possession of the miller694u@gmail.com email account or the external hard drive. Accordingly, the

evidence presented at trial was insufficient to support a finding beyond a reasonable doubt that Miller, rather than Fred, received, distributed, and possessed child pornography. Assuming *arguendo* that this Court finds Miller's statements relevant to the possession count, the distribution and receipt counts should still be separately analyzed in light of the ample evidence establishing shared access to the miller694u@gmail.com email account. As such, Miller's convictions should be reversed, and his case remanded for a new trial.

## CONCLUSION

For the reasons stated above, and the reasons detailed in Miller's opening brief, Miller requests this Court reverse his conviction for all counts.

Respectfully submitted,

/s/ Eric G. Eckes
ERIC G. ECKES (Ky. Bar No. 93604)
(CJA Appointed)
Pinales, Stachler, Young, Burrell & Crouse Co., LPA
455 Delta Ave., Suite 105
Cincinnati, Ohio 45226
(513) 252-2723
(513) 252-2751
eeckes@pinalesstachler.com

## CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing has been served via this Court's ECF system to:

Charles P. Wisdom Jr.
U.S. Attorney's Office
260 W. Vine Street
Suite 300
Lexington, KY 40507

on this 18th day of January, 2019.

/s/ Eric G. Eckes
ERIC G. ECKES (Ky. Bar No. 93604)
Counsel for Defendant-Appellant

## CERTIFICATE OF COMPLIANCE

This brief has been prepared using 14-point proportionally spaced font.

Exclusive of the table of contents, table of authorities, the certificate of service, and certificate of compliance, the brief contains 4,221 words.

I understand that material representations can result in the Court's striking of the brief and imposing sanctions. If the Court so directs, I will provide an electronic version of the brief and/or copy of the word or line printout.

/s/ Eric G. Eckes