



THE JOURNAL OF
**DIGITAL FORENSICS,
SECURITY AND LAW**

**Journal of Digital Forensics,
Security and Law**

Volume 17

Article 3


1-14-2022

Digital Evidence In Appeals Of Criminal Cases Before The U.S. Courts Of Appeal: A Review Of Decisions And Examination Of The Legal Landscape From 2016 – 2020

Martin Novak

National Institute of Justice, martin.novak@usdoj.gov

Follow this and additional works at: <https://commons.erau.edu/jdfsl>

 Part of the [Computer Law Commons](#), [Criminal Law Commons](#), [Information Security Commons](#), and the [Jurisprudence Commons](#)

Recommended Citation

Novak, Martin (2022) "Digital Evidence In Appeals Of Criminal Cases Before The U.S. Courts Of Appeal: A Review Of Decisions And Examination Of The Legal Landscape From 2016 – 2020," *Journal of Digital Forensics, Security and Law*. Vol. 17 , Article 3.

Available at: <https://commons.erau.edu/jdfsl/vol17/iss1/3>

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.



(c)ADFSL



Digital Evidence In Appeals Of Criminal Cases Before The U.S. Courts Of Appeal: A Review Of Decisions And Examination Of The Legal Landscape From 2016 – 2020

Cover Page Footnote

The author thanks Danielle Crimmins, Ph.D. for her comments on earlier drafts of this work.

DIGITAL EVIDENCE IN APPEALS OF CRIMINAL CASES BEFORE THE U.S. COURTS OF APPEAL: A REVIEW OF DECISIONS AND EXAMINATION OF THE LEGAL LANDSCAPE FROM 2016 – 2020*

Martin Novak

National Institute of Justice
martin.novak@usdoj.gov

ABSTRACT

This study is a follow-up to Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration – 2010 to 2015. The current study examines appeals of criminal cases before the United States Courts of Appeal from January 2016 through August 2020, where one or more appeal claims were related to digital evidence. The purpose of this research was to determine if the legal landscape has changed since 2015; examine the most relevant legal issues related to digital evidence; and analyze how precedential cases may have affected digital forensics as evidence.

Keywords: Digital Evidence, Compelled Decryption, Geo-Location, Network Investigative Technique, Border Searches, U.S. Courts of Appeal

1. INTRODUCTION

Results from the study Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration (2010 – 2015)¹ showed that the majority of appeals involving digital evidence included in the study were for offenses related to child pornography – over 90%. The remaining ten percent were offenses related to narcotics, sex

crimes, weapons, violent crimes, and white collar crimes. Similarly, the majority of digital evidence involved came from the hard drives of suspect's computers or laptops – over 85%. The remaining evidence was from cell phones, GPS tracking devices, and digital cameras.

New types of digital technologies have emerged since 2015, introducing new challenges for investigators in capturing and acquiring digital evidence. We live in a world that is more connected to the Internet than ever before. We connect through our computers, our smartphones, and wearable devices – The number of smartphone users worldwide

*PERIOD COVERED INCLUDES JANUARY 2016 – AUGUST 2020.

¹Martin Novak, "Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration," *Journal of Digital Forensics, Security and Law* 14, no. 4 (April 2020), <http://commons.erau.edu/jdfs1/vol14/iss4/3>.

since 2017 has jumped from 2.9 billion to 3.5 billion in 2020.²

Border crossings create an interesting use case scenario for the searching and seizing of electronic devices. On a typical day in 2019, approximately 1,124,000 people entered through the United States' borders by plane, automobile, ship, and on foot.³ With recent estimates stating that 44.87% of people in the world own a smartphone,⁴ then over 500,000 people entering the United States every day likely have a smartphone.

The duties of the U.S. Customs and Border Protection Agency include stemming the flow of illegal drugs and other contraband, including digital contraband. That contraband may contain evidence of criminal activity, such as drug trafficking, human trafficking, and possession of child pornography. Determining which of those are likely to possess some form of digital contraband is difficult enough. Further deducing which of those to search is even more daunting.

From marketplaces specializing in the sale and distribution of controlled substances, to a proliferation of child pornography, the Dark Net provides a host of potential criminal activity. The encrypted nature of TOR, the perceived anonymity it provides, and the cryptocurrency used for illicit transactions create a host of barriers for law enforcement to investigate crimes committed on the Dark Net.

²Statista, "Number of Smartphone Users from 2016 to 2021," Statista, last modified November 2020, accessed November 19, 2020, <https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/>.

³U.S. Customs and Border Patrol, "On a Typical Day in Fiscal Year 2019," U.S. Customs and Border Protection Agency, last modified April 15, 2020, accessed November 19, 2020, <https://www.cbp.gov/newsroom/stats/typical-day-fy2019>.

⁴Ash Turner, "Number Of Smartphone Mobile Phone Users Worldwide," Bank My Cell (blog), entry posted November 2020, accessed November 19, 2020, <https://www.bankmycell.com/blog/how-many-phones-are-in-the-world>.

Nearly every one of these investigations involves the acquisition and analysis of digital evidence.

A recent success for law enforcement was the FBI's Operation Pacifier, an investigation of Playpen, a Dark Net child pornography sharing web site. The results for Operation Pacifier were staggering. In the United States alone, there were 350 arrests and 76 successful prosecutions. Internationally, 296 victims of abuse were rescued or identified, along with 548 arrests, based on the intelligence gathered through Operation Pacifier.⁵ While this was all very good news for the criminal justice community, the sobering reality is that similar sites continue to occupy corners of the dark net.

The use of end-to-end encryption in communication and the full-disk encryption of mobile devices place sometimes impenetrable roadblocks for law enforcement lawful access to communications and data. According to one report, if Apple and Google fully implement full disk encryption, 99 percent of smartphones in the world may become inaccessible.⁶ This creates a situation where even with a valid search warrant, law enforcement is often unable to acquire evidence that they are legally entitled to obtain.

1.1 Structure

In an effort to address these challenges, the goals of the current study are twofold: It first reviews appeals in criminal cases before the United States Courts of Appeal relating to digital evidence from 2016 – 2020. Second is a review of the jurisprudence affecting decisions

⁵"Playpen' Creator Sentenced to 30 Years," news release, May 5, 2017, accessed November 26, 2019, <https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years>.

⁶James A. Lewis, Denise E. Zheng, and William A. Carter, *The Effect of Encryption on Lawful Access to Communications and Data* (Washington, DC: Center for Strategic International Studies, 2017), iv.

made in appeals involving some aspect of digital evidence across the legal landscape.

Section two reviews appeals of criminal cases before the United States Courts of Appeal from 2016 to August 2020 and presents the findings and discussion. Section three examines the jurisprudence related to digital evidence, including the associated legal issues affected, constitutional rights implicated, and current scholarly opinion on these matters. Section four discusses the limitations of this study, while section five presents the study's conclusions.

2. APPEALS IN CRIMINAL CASES BEFORE THE UNITED STATES COURTS OF APPEAL (2016 – 2020)

This section is a review of appeals of criminal cases before the United States Courts of Appeal from 2016 to August 2020 involving digital evidence. The two main goals of the review were to explore how digital evidence has changed since 2015, and examine how digital evidence has withstood challenges on appeal since 2015.

2.1 Research Questions

A retrospective study was undertaken as a follow on to the author's previous research,⁷ seeking answers to the following questions:

- How well has digital evidence withstood challenges on appeal?
- How frequently are decisions affirmed for the defense?

⁷See Martin Novak, "Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration," *Journal of Digital Forensics, Security and Law* 14, no. 4 (April 2020): accessed September 16, 2020, <http://commons.erau.edu/jdfsl/vol14/iss4/3>.

- What is the most frequently occurring basis of appeal?
- What is the most common legal basis for appeals related to some aspect of digital evidence? The current research sought answers to the following research questions and compares the answers to the author's previous work:
- What are the most common offenses related to digital evidence?
- What are the most common types of evidence?

Finally, this study looks at the current legal landscape for digital evidence to understand it may affect appeals related to digital evidence going forward.

2.2 Methodology

The following analysis is based on relevant appeals of criminal cases before the United States Courts of Appeal from 2016 – August 2020 involving some aspect of digital evidence. Civil appeals were not included as part of this study.

2.2.1 Data and Search Terms

Data for this project was drawn from appeals of criminal cases that were affirmed or reversed by the United States Courts of Appeal for the period 2015 – 2020. Cases were identified via LexisNexis, using the following search terms: *Probable Cause, Encryption, GPS, Geolocation, Geo-Fence, Onion Router, Wearables, Internet of Things, Text Message, Cryptocurrency, Network Investigative Tool (NIT), Particularity, Cell Phone, Metadata, Digital Evidence, Dark Web, ECPA, Social Media, CSLI, and Child Pornography*.⁸

⁸Search terms in the previous study included Computer, Computer Forensics, Chat Log, Electronic Evidence, Cell Phone, Sexting, iPhone, Child Pornography, Digital Evidence, Computer Investigation, GPS, and Encryption.

2.3 Results and Discussion

The search terms used identified 112 appeals where the legal issues involved digital evidence in appeals of criminal cases before the United States Courts of Appeal between 2016 and 2020. Those appeals resulted in 108 judgments (96.43%) that were affirmed or reversed for the government.⁹ This success rate is even better than the general success rate for the government for all criminal cases heard before the U.S. Courts of Appeal for the same time period – 90.9%.¹⁰ However, it should be noted that many factors are in play in the appeals of criminal cases, including the type of crime, type of harm inflicted, and sentence imposed by District Court.

2.3.1 Decisions Affirmed for the Defense

Four appeals were affirmed for the defense, and zero appeals were reversed for the defense. Of those appeals, two were based on probable cause, one on relevancy, and one on scientific merit.

2.3.2 Most Frequently Occurring Bases of Appeal

There were 79 appeals based on Probable Cause, as the most frequently occurring basis for appeal. There were 15 appeals based on Sufficiency of Evidence, eight appeals based on Scientific Merit, five based on Probative Value. Finally, a combined five appeals were based on Relevancy or Authenticity. No ap-

⁹Affirmed means that the court of appeals has concluded that the lower court decision is correct and will stand as rendered by the lower court. Reversed is the act of a court setting aside the decision of a lower court (often accompanied by a remand to the lower court for further proceedings)

¹⁰A subsequent search of Lexis Nexis showed that there was no subsequent history for any of the cases included in this study. In several instances US Supreme Court certiorari was denied, but the outcomes for all appeals were unchanged.

peals based on Hearsay or Best Evidence were identified as a basis of appeal in this study.

2.3.3 Offenses Related to Digital Evidence

The offenses associated with these appeals ran the breadth of criminal activity. There were 44 offenses related to child pornography, including production, possession, and distribution were the most frequently occurring basis of appeal. There were 34 narcotics related offenses, including distribution and possession. There were 17 violent offenses, including murder, manslaughter, and cyberstalking. There were nine sex offenses, including enticement, exploitation, and prostitution. Additionally, there were five white collar offenses, including fraud and tax evasion. Finally, there were three offenses related to illegal weapons possession and distribution.

Table 1 is a comparison between the two time periods, showing that most offenses are still related to child pornography for the period 2016 – 2020. There were considerably more offenses related to narcotics, violent crimes, and sex crimes. White collar offenses and weapons offenses did not change appreciably.¹¹

2.3.4 Types of Evidence - Comparison

In figure 2, cell phones were the most numerous type or piece of evidence at 52, while evidence from IP-addresses came in next at twenty-nine. The third most numerous piece of evidence was computers at 20, with Bit-

¹¹Narcotics-related offenses included trafficking, possession, and production. Child pornography offenses included possession, production, and distribution. Violent crime offenses included homicide, manslaughter, extortion, armed robbery, cyberstalking, arson, kidnapping, and terrorism. Sex crimes included enticement, exploitation, and sex trafficking. White collar crimes included tax evasion, and obstruction of justice,

Offenses	2010-2015	2016-2020
Child Pornography	132	44
Narcotics	5	34
Violent Crimes	1	17
Sex Crimes	2	9
White Collar	5	5
Weapons	1	3
Totals	146	112

Table 1. Comparison of Offenses

Evidence	2010-2015	2016-2020
Cell Phone	5	51
IP Address	-	29
Computer ¹²	125	20
GPS	4	9
Bitcoin	-	3
External Media	11	-
Digital Camera	1	-
Totals	146	112

Table 2. Comparison of evidence types

coin and GPS devices combining for 13 pieces of evidence.

In comparing the types of digital evidence from the first study to the current one, it is interesting to note that the addition of IP-addresses as evidence in the current study, while no occurrences of this type of evidence appeared in the study that covered 2010 – 2015. Also, cell phones have become the dominant type of evidence seen in these appeals.¹³ This will likely continue to be the case as our society becomes more mobile and dependent upon these types of devices.

3. LEGAL LANDSCAPE

This section is a review of the jurisprudence affecting decisions made in appeals involving some aspect of digital evidence across the legal landscape. Four areas of jurisprudence

¹³The category cell phone included text based cellular phones and smart phones.

related to digital evidence have come to the forefront of the legal landscape since 2015 – Border Searches of Electronic Devices, Compelled Decryption of Digital Devices, Network Investigative Technique (NIT) Warrants, and Geo-fence Warrants. For each of these theories of law, the associated legal issues affected and constitutional rights implicated are examined. Note that the cases cited in this section are not necessarily part of the cases reviewed included in the review of appeals that were part of this study. Rather, they address the development of the jurisprudence over time for each area of the legal landscape.

3.1 Border Searches of Electronic Devices

The Fourth Amendment to the United States Constitution guarantees 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, describing the place to be searched with particularity, and the persons or things to be seized.

Two centuries of jurisprudence have delineated what the founding fathers meant by the terms unreasonable, particularity, and probable cause. Along those same lines has been the development of the doctrine of the Border Search Exception, where searches conducted at our nation's borders do not require probable cause. Before delving into the Border Search Exception, we should be clear about the difference between the terms "reasonable suspicion" and "probable cause." Reasonable suspicion is "an objectively justifiable suspicion that is based on specific facts or circumstances that justifies stopping and sometimes searching (as by frisking) a person thought

to be involved in criminal activity at the time."¹⁴

For a more invasive search or to obtain an arrest warrant, probable cause is required. Probable cause is "sufficient reason based upon known facts to believe a crime has been committed or that certain property is connected with a crime."¹⁵

The Border Search Exception doctrine has seen its own refinement over time as circumstances and situations have required it to. In 1971, Customs agents seized illicit photos from Milton Luros at Los Angeles International Airport. Luros argued that the search was unreasonable because there was no predicate probable cause to conduct the search.

Ruling in favor of the government, the Supreme Court declared, "A port of entry is not a traveler's home. His right to be let alone neither prevents the search of his luggage nor the seizure of unprotected, but illegal, materials when his possession of them is discovered during such a search. Customs officials characteristically inspect luggage, and their power to do so is not questioned in this case; it is an old practice and is intimately associated with excluding illegal articles from the country."¹⁶

In a similar case two years later, in a case involving reels of film containing pornography, the Supreme Court affirmed that "Import restrictions and searches of persons or packages at the national borders rest on different

considerations and different rules of constitutional law from domestic regulations."¹⁷

Finally, in a 1977 appeal involving a mail order drug business, the Supreme Court found that Customs Agents acted reasonably, stating that "border searches, then, from before the adoption of the Fourth Amendment, have been considered to be 'reasonable' by the single fact that the person or item in question had entered into our country from outside. There has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause. This longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless 'reasonable' has a history as old as the Fourth Amendment itself."¹⁸

While these rulings seemed to satisfy most situations in a pen and paper world, the dawn of the digital age has brought the question of what constitutes a "reasonable" search of electronic devices at the border into question. The Supreme Court has yet to make a definitive ruling to date. Rather, the U.S Courts of Appeal have been left to their own devices, with the Fourth and Eleventh Circuit coming to different conclusions.

3.1.1 Fourth Circuit Court of Appeals

On February 2, 2016, Hamza Kolsuz was detained at Washington Dulles International Airport while attempting to board a flight to Turkey after federal customs agents found firearms parts in his luggage. Kolsuz had been part of an ongoing investigation into arms smuggling by the Customs and Border Protection Agency (CBP).

After arresting Hamza Kolsuz on charges of arms smuggling, CPB agents took posses-

¹⁴Thomson Reuters, "Reasonable Suspicion," Find-Law Legal Dictionary, last modified 2020, accessed October 19, 2020, <https://dictionary.findlaw.com/definition/reasonable-suspicion.html>.

¹⁵Gerald Hill and Kathleen Hill, "Probable Cause," The People's Law Dictionary, last modified 2020, accessed October 19, 2020, <https://dictionary.law.com/Default.aspx?selected=1618>.

¹⁶United States v. Thirty-seven Photographs, 402 U. S. 363, 376 (1971)

¹⁷United States v. 12 200-Ft. Reels of Film, 413 U. S. 123, 125 (1973)

¹⁸United States v. Ramsey et al., 431 U.S. 606 (1977)

sion of his smartphone and subjected it to a month-long, off-site forensic analysis, yielding a nearly 900-page report cataloging the phone's data. Prior to his trial, Kolsuz moved to suppress the forensic report on his phone by arguing that the border exception did not apply to the search. The district court denied this motion, finding that the search was reasonable under the Fourth Amendment. Kolsuz ultimately was convicted of attempting to smuggle firearms out of the country and an associated conspiracy charge and sentenced to 30 months incarceration.

On appeal, Kolsuz contended that once both he and his phone were in government custody, the government interest in preventing contraband from crossing the border was no longer implicated, so the border exception should no longer apply. Second, relying chiefly on *Riley v. California*, 134 S. Ct. 2473 (2014) (holding that search incident to arrest exception does not apply to searches of cell phones), Kolsuz urged that "the privacy interest in smartphone data is so weighty that even under the border exception, a forensic search of a phone requires more than reasonable suspicion, and instead may be conducted only with a warrant based on probable cause."¹⁹

The panel from the Fourth Circuit affirmed the district court's ruling, saying that "despite the temporal and spatial distance between the off-site analysis of the phone and Kolsuz's attempted departure at the airport, the justification for the border exception is broad enough to reach the search in this case."²⁰ The panel said further that "it was reasonable for the officers who conducted the forensic analysis of the phone to rely on the established and uniform body of precedent allowing warrantless border searches of digital

devices that were based on at least reasonable suspicion."²¹

3.1.2 Eleventh Circuit Court of Appeals

On December 21, 2014, Karl Touset arrived at the international terminal at Hartsfield-Jackson Atlanta International Airport, where CBP agents detained him. Following an inspection of his luggage, the CBP agents allowed Touset to leave. However, they retained several of his electronic devices for further examination. The subsequent forensic searches revealed child pornography on two laptops and two external hard drives. On January 28, 2015, following a search of his home in Marietta, Georgia, Touset was arrested and charged with possession of child pornography.

Prior to trial, Touset filed a motion at an evidentiary hearing before the magistrate judge to suppress the evidence found on his devices seized at the border. He argued that the search was based on a warrant that was stale, and the CBP did not have reasonable suspicion to conduct the search. The magistrate judge found that CBP agents had reasonable suspicion, and the warrant was not stale because "files on a computer are less likely than other types of contraband to disappear over time and can often be recovered even if they are deleted."²²

At trial, the district court adopted the magistrate's ruling, finding that "that reasonable suspicion existed for the detention and forensic search of Touset's electronic devices."²³ Touset subsequently pled guilty to possession of child pornography and was sentenced to 120 months of imprisonment. He appealed his conviction to the United States Court of Appeals, Eleventh Circuit.

¹⁹ *United States v. Kolsuz*, 890 F.3d 133, 132 (4th Cir. 2018).

²⁰ *Id.*, 133.

²¹ *Id.*, 133.

²² *United States v. Touset*, 890 F.3d 1227, 1231 (11th Cir. 2018).

²³ *Id.*, 1231

On May 23, 2018, the panel from the 11th Circuit affirmed Touset's sentence. Finding that reasonable suspicion was not required to conduct a search at the border, the panel said that "we see no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property. Just as the United States is entitled to search a fuel tank for drugs, it is entitled to search a flash drive for child pornography."²⁴

The panel also found that the warrant upon which the search was based was not stale because "the evidence that Touset made three separate payments to the Western Union account associated with the Philippine phone number was not stale about a year and a half later. That evidence suggested that Touset likely received child pornography electronically and had child pornography stored on his electronic devices."²⁵

In the end, it does not seem to matter whether or not reasonable suspicion is required to conduct an invasive search of electronic devices at our nation's borders. Any further clarification on this point will likely come from a United States Supreme Court ruling, or legislation directly addressing the search of electronic devices at the border.

3.1.3 Reasonable Suspicion or Probable Cause?

The debate on searches of electronic devices at the nation's borders focuses on the legal issues of reasonable suspicion, probable cause, and implicates protections against unreasonable search and seizure guaranteed by the Fourth Amendment, and seeks answers to the following questions:

- Is a search warrant based on probable cause required for an invasive search of

electronic devices at our nation's borders?

- Or, is reasonable suspicion sufficient to conduct an invasive search?

Soder (2019) contends that "the reasonable suspicion standard achieves the appropriate balance, ensuring law-abiding travelers need not worry about being subjected to an intrusive search of their electronic devices and sensitive digital information."²⁶

Referring to recent decisions in *Riley and Carpenter*, Gomez (2020) argues that the Supreme Court "should decide the circuit split . . . and conclude that the Fourth Amendment requires government agents to have individualized "reasonable suspicion" prior to conducting forensic searches of electronic devices at the border."²⁷

Bohannon (2019) contends that probable cause is the correct standard to apply for searches of digital devices at the border. In *Cell Phones and the Border Search Exception*, she states that "international travel . . . should not provide a loophole to Fourth Amendment protections and allow the government to seize personal information unrelated to the justifications embedded in general sovereignty interests at the border."²⁸ Bohannon concludes by saying that "requiring a warrant supported by probable cause for cell phone searches at the border is an

²⁶Michael Soder, "A Constitutional Limbo: Searches of Electronic Devices at the International Border," *University of Cincinnati Law Review* 88, no. 1 (2019): 270.

²⁷Ashley N. Gomez, "Over the Border, under What Law: The Circuit Split over Searches of Electronic Devices on the Border," *Arizona State Law Journal* 52, no. 1 (Spring 2020): 310.

²⁸Gina R. Bohannon, "Cell Phones and the Border Search Exception: Circuits Split over the Line between Sovereignty and Privacy," *Maryland Law Review* 78, no. 3 (2019): 599.

²⁴Id, 1233

²⁵Id, 1234

administrable requirement that adequately protects privacy interests."²⁹

Citing the inadequacies of the *Kolsuz and Tousef* decisions, DeLorimer (2019) agrees with Bohannon, saying that "although an individualized suspicion standard is a step in the right direction, the court missed an opportunity to hold that a warrant is required prior to conducting a forensic border search of a cell phone. Thus, until the Supreme Court rules on the matter, the status of international airline travelers' digital privacy is up in the air because of this circuit split."³⁰

Further complicating matters with regard to border searches of electronic devices is the matter of routine versus non-routine searches. A routine search is conducted when there is no reasonable suspicion that the item being searched contains evidence of criminal or illegal activity. This is analogous to what we do as travelers when we go through routine airport security. A non-routine search, on the other hand, involves "a high degree of personal intrusion-such as a strip search-requires "reasonable suspicion, which calls for some particularized and objective basis for suspecting wrongdoing."³¹ This would be akin to being detained after passing through routine airport security.

For their part, the U.S. Customs and Border Protection Agency has clarified what it considers a non-routine search versus a routine search of an electronic device. Issued in 2018, the agency's guidance states that "instances in which there is reasonable suspicion of activity in violation of the laws enforced

or administered by CBP . . . an Officer may perform an advanced search of an electronic device."³²

The guidance goes on to describe an advanced (non-routine) search as "any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and analyze its contents."³³

Meade (2020) contends that all forensic searches of electronic devices at the border are non-routine and that the Supreme Court should "require a warrant supported by probable cause of criminality before searching electronics seized at the border."³⁴ O'Grady (2019) concludes this discussion by saying that it "seems increasingly likely that the Supreme Court will need to resolve how the border search exception applies to government searches of electronic devices."³⁵

3.2 Compelled Decryption of Digital Devices

Today, the majority of Americans own a cell phone. According to Pew Research, 96% own a cell phone, and of those, 81% own a smartphone. A smartphone's capability of locking with an alphanumeric code, or biometric such as a fingerprint, eye scan, facial recognition is central to the discussion of compelled decryption.

The Fifth Amendment to the United States Constitution protects a witness from being compelled to give self-incriminating testi-

²⁹Bohannon, "Cell Phones," 602.

³⁰Andrea DeLorimer, "Flying in the Face of Suspicionless Cell Phone Searches: Fourth Circuit Grants Airline Passengers Heightened Protection from Searches by Customs Officers," *Journal of Air Law and Commerce* 84, no. 1 (2019): 134.

³¹Sean O'Grady, "All Watched over by Machines of Loving Grace: Border Searches of Electronic Devices in the Digital Age," *Fordham Law Review* 87, no. 5 (April 2019): 2265.

³²Kevin McAleenan, *Border Search of Electronic Devices*, publication no. 3340-049A (Washington, DC: U.S. Customs and Border Protection, 2018), 4-5.

³³McAleenan, *Border Search*, 4-5.

³⁴Chloe Meade, "The Border Search Exception in the Modern Era: An Exploration of Tensions between Congress, the Supreme Court, and the Circuits," *Boston University Journal of Science and Technology Law* 26, no. 1 (2020): 194.

³⁵O'Grady, "All Watched," 2284

mony. Two terms from jurisprudence define the discussion concerning compelled decryption – Testimonial and Non-Testimonial. If a witness or suspect is forced to produce the "contents of one's own mind," it is considered testimonial and therefore protected by the Fifth Amendment.

If on the other hand, what the witness or suspect is forced to produce is a foregone conclusion, such as a fingerprint, then it is considered non-testimonial and not protected by the Fifth Amendment. To claim a foregone conclusion, "the government must be able to establish its prior knowledge of the existence, possession, and authenticity of the requested documents with "reasonable particularity."³⁶

Recent court rulings demonstrate that there is a divergence of opinion of when compelling decryption becomes testimonial. In *United States v. Doe (In re Grand Jury Subpoena Duces Tecum)*³⁷, 670 F.3d 1335 (11th Cir. 2012), the 11th circuit held that the requirement "to use a decryption password is most certainly more akin to requiring the production of a combination because both demand the use of the contents of the mind, and the production is accompanied by . . . implied factual statements . . . could prove to be incriminatory."³⁸ In this instance, producing a password was considered testimonial. In *State v. Diamond*, 905 N.W.2d 870; (MN, 2018), the Court of Appeals of Minnesota ruled that ordering the "appellant to provide a fingerprint to unlock a seized cell-

³⁶Richard M. Thompson, II and Chris Jaikaran, Encryption: Selected Legal Issues, issue brief no. R44407 (Washington, DC: Congressional Research Service, 2016), 14.

³⁷A subpoena duces tecum requires the witness to produce a document or documents pertinent to a proceeding. From the Latin duces tecum, meaning "you shall bring with you".

³⁸*United States v. Doe (In re Grand Jury Subpoena Duces Tecum)*, 670 F.3d 1335, 1346 (11th Cir. 2012).

phone did not violate his Fifth Amendment privilege against self-incrimination because of the compelled act as not a testimonial communication."³⁹ On this occasion, providing a fingerprint was considered non-testimonial.

Recently, in *re Search of a Residence in Oakland*, 354 F. Supp. 3d 1010 (N.D. Cal. 2019), the United States District Court for the Northern District of California declared that a "finger or thumb scan used to unlock a device indicates that the device belongs to a particular individual. In other words, the act concedes that the phone was in the possession and control of the suspect, and authenticates ownership or access to the phone and all of its digital contents."⁴⁰ In this case, providing a fingerprint was considered testimonial. Clearly, this ruling is counter to *State v. Diamond*, so the ultimate determination on compelled decryption has yet to be made. In all likelihood, it will be left to the United States Supreme Court to determine the rules for compelling decryption of electronic devices.

3.2.1 The Contents of One's Own Mind or a Foregone Conclusion?

The discussion among scholars on the compelled decryption of digital devices centers around the following questions:

- Does the act of compulsion force a suspect or witness to reveal the contents of his mind, making the statement testimonial?
- Or, is the act of compulsion merely a foregone conclusion, rendering the statement non-testimonial?

³⁹US Supreme Court certiorari denied by *Diamond v. Minnesota*, 2018 U.S. LEXIS 3071 (U.S. 2018).

⁴⁰*In re Search of a Residence in Oakland*, 354 F. Supp. 3d 1010, 1016 (N.D. Cal. 2019)

- In either scenario, can the witness or suspect claim Fifth Amendment privilege against self-incrimination?

Scholars like Metz (2019) contend that protection from compulsion in the digital age is essential to protecting the privilege against self-incrimination provided by the Fifth Amendment. Metz argues that "allowing authorities to force the production of a device and its contents via the compulsion of biometric data brushes dangerously close to an inquisitorial system of justice."⁴¹

Other scholars, like Reitingger (2019) concur, stating that "compelled device unlock based on a fingerprint or facial scan should be deemed to infringe upon the Fifth Amendment's protection against self-incrimination."⁴²

Kerr (2019) compares the search of a digital device with encryption to the traditional search of a dwelling. With a valid search warrant, officers may conduct a search of the entirety of the dwelling, detain any persons in the dwelling, and search any place in the dwelling where they may find evidence as particularized in the search warrant. In contrast, digital devices, particularly cell phones, are encrypted creating as Kerr describes it inserting "a door in front of many forms of electronic treasure."⁴³

According to Kerr, the answer to greater access to information on cell phones is not a Fifth Amendment problem. Although the Fourth Amendment may protect the contents

of the cell phone, "Proof of ability to enter in the password disarms the privilege against self-incrimination by rendering the testimonial aspect of production-knowledge of the password-a foregone conclusion."⁴⁴

Contending that compelled decryption raises Fourth and Fifth Amendment issues, Chase (2020) says that "the courts could ensure that individual rights, especially in regard to digital devices and the biometric locks that are so commonly used with them, are fundamentally protected at a time when technology could allow government power to grow exponentially."⁴⁵ He argues this would not end law enforcement's ability to find evidence on digital devices. Instead, Chase says it would mean "that law enforcement must consider the conditions required for two amendments instead of one."⁴⁶

Suggesting that we should consider the right to go dark, Gray (2019) states that "recognizing a right to go dark would guarantee our authority to determine whether our devices can testify against us. If that were the law, then a derivative right to go dark would guarantee that nothing our devices know as a consequence of being our devices could ever be used against us unless we affirmatively waived."⁴⁷

While Gray says that there is a case to be made for a limited right to go dark for devices covered by doctor-patient privileges or medical monitoring devices subject to HIPAA privacy laws, "there does not seem to be good grounds for a general right to go dark when it

⁴¹Howard Metz, "Your Device Is Disabled: How and Why Compulsion of Biometrics to Unlock Devices Should Be Protected by the Fifth Amendment Privilege," *Valparaiso University Law Review* 53, no. 2 (Winter 2019): 466.

⁴²Nathan Reitingger, "Faces and Fingers: Authentication," *Journal of High Technology Law* 20, no. 1 (2020): 62.

⁴³Orin S. Kerr, "Compelled Decryption and the Privilege against Self-Incrimination," *Texas Law Review* 97, no. 4 (March 2019): 795.

⁴⁴Kerr, "Compelled Decryption," 799

⁴⁵Aaron Chase, "Secure the Smartphone, Secure the Future: Biometrics, Boyd, a Warrant Denial and the Fourth and Fifth Amendments," *Hastings Race and Poverty Law Journal* 17, no. 2 (Summer 2020): 603.

⁴⁶Chase, "Secure the Smartphone," 603.

⁴⁷David Gray, "A Right to Go Dark," *SMU Law Review* 72, no. 4 (Fall 2019): 667.

comes to personal electronic devices adopted by users on their own initiative."⁴⁸

3.3 Network Investigative Technique (NIT) Warrants

The *Particularity* requirement of the *Fourth Amendment* specifies that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.

The *Good Faith Exception* is an advancement in exclusionary rule, promulgated in *the United States v. Leon*, 468 U.S. 897 (1984). In this ruling, the Supreme Court held that the Fourth Amendment exclusionary rule should not be applied so as to bar the use in the prosecution's case in chief of evidence obtained by officers acting in reasonable reliance on a search warrant issued by a detached and neutral magistrate but ultimately found to be invalid.⁴⁹

If the court finds that an officer did not act in good faith or that the warrant was not particularized, the warrant's validity could be called into question. These issues came under the scrutiny of the courts in recent cases related to the Federal Bureau of Investigation's (FBI) *Playpen* investigation.

In August, 2014, the dark net site, *Playpen* was launched to distribute child pornography and offering advice on grooming and avoiding detection. Within a month, *Playpen* had over 60,000 registered users, with an average of 11,000 visits per week. In January 2015, the FBI seized the server hosting the site, which was located in Lenoir, North Carolina. The FBI did not immediately shut down the site.

Instead, the FBI obtained a search warrant that authorized them to run the site

as a honeypot from February 20, 2015, to March 4, 2015. This was Operation Pacifier. The purpose of the honeypot⁵⁰ was for the FBI to deploy a Network Investigative Tool (NIT). The FBI used the NIT pursuant to a warrant it obtained from a magistrate judge in the Eastern District of Virginia (the NIT warrant).⁵¹

Once a user requested a download of child pornography from the *Playpen* site, the NIT sent the user's computer a piece of code. That piece of code returned the following information to law enforcement: the requesting computer's actual IP address and the date and time that the NIT requested this information; a unique identifier for that particular requesting computer; the type of operating system running on the computer; the requesting computer's Host Name (i.e., "Fred's Computer"); the requesting computer's username; and the requesting computer's media access control (MAC) address.

Based on the information obtained from the NIT, law enforcement obtained a valid search warrant based on probable cause that the individual was actively engaged in the possession and/or distribution of child pornography. As a result of *Operation Pacifier*, one of those arrested was Alex Levin. On a subsequent warrant, the FBI searched Alex Levin's home in Norwood, Massachusetts, on September 17, 2015. Finding images and videos containing child pornography, Levin was indicted and charged with possession of child pornography. Levin immediately moved to suppress the evidence obtained from the NIT warrant and the subsequent warrant issued in Massachusetts.

In a potentially devastating ruling for the government, the United States District Court

⁴⁸Gray, "A Right to Go Dark," 668.

⁴⁹United States v. Leon, 468 U.S. 897, 905 (1984).

⁵⁰A honeypot website is meant to capture users that are attracted to the illicit content that site may provide.

⁵¹United States v. Levin, 874 F.3d 316, 317 (1st Cir. Oct. 27, 2017).

for the District of Massachusetts granted Levin's motion. Citing *United States v. Krueger*, 809 F.3d 1109 (10th Cir. 2015), the court ruled that "since the warrant purported to authorize a search of property located outside the federal judicial district where the issuing judge sat, the NIT warrant was issued without jurisdiction and thus was void ab initio."⁵²⁵³ They further ruled that the resulting search was invalid since the magistrate was not authorized to issue the NIT warrant. The good faith exception did not apply because the court found the NIT warrant to be void ab initio. The government appealed this ruling to the United States Court of Appeals for the First Circuit.

Amid the challenges in court to the NIT warrant by Levin and others, the U.S. Supreme Court amended Rule 41(b) that addresses the venue for a warrant application. On February 20, 2015, when the NIT Warrant was issued, Rule 41(b)(1) stated that

At the request of a federal law enforcement officer or an attorney for the government: (1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district.⁵⁴

This meant that a magistrate could only sign search warrants associated with suspected crimes in the territory covered by the district in which they operated. Clearly, many of the suspects arrested in connection with the Playpen case lived outside of the Eastern District of Virginia, where the NIT

warrant was approved. The change to Rule 41(b) approved by Congress and the U.S. Supreme Court in April 2016, added the following language:

41(b)(6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if: (A) the district where the media or information is located has been concealed through technological means.⁵⁵

The U.S. Department of Justice supported the amendment to Rule 41(b) because they believed that "technology should not create a lawless zone merely because a procedural rule has not kept up with the times."⁵⁶ Department officials insisted that the amendment did not change any of the requirements under the Fourth Amendment for establishing probable cause in an application for a warrant. Rather, the new amendment would do "what the Rules were always intended to do: identify a judge who can consider whether to grant or deny a warrant application."⁵⁷

On October 27, 2017, the First Circuit panel reversed the District Court's findings in their entirety. With regard to the particularity of the NIT warrant, the panel found that it "clearly specifies that only activating computers – that is "those of any user . . . who logs into [Playpen] by entering a username and password"⁵⁸ – are to be searched.

⁵⁵Id., 53.

⁵⁶Leslie R. Caldwell, "Ensuring Tech-Savvy Criminals Do Not Have Immunity from Investigation," DoJ - Office of Public Affairs (blog), entry posted November 21, 2016, accessed September 8, 2020, <https://www.justice.gov/archives/opa/blog/ensuring-tech-savvy-criminals-do-not-have-immunity-investigation>.

⁵⁷Id.

⁵⁸United States v. Levin, 874 F.3d 316, 323 (1st Cir. 2017).

⁵²United States v. Levin, 186 F. Supp. 3d 26, 35 (D. Mass., Apr. 20, 2016)

⁵³The term void ab initio means "to be treated as invalid from the outset"

⁵⁴Federal Rules of Criminal Procedure, C.F.R. (2018). Accessed October 1, 2020. https://www.uscourts.gov/sites/default/files/criminal-rules-procedure-dec2017_0.pdf, 53.

The NIT warrant specifies into which homes an intrusion is permitted (those where the activating computers are located), and on what basis (that the users in those homes logged into Playpen).⁵⁹

Finding that the executing officers acted in good faith, the panel further concluded that the “warrant, in this case, was particular enough to infer that, in executing it, the [executing officers] act[ed] with an objectively reasonable good-faith belief that their conduct [was] lawful.”⁶⁰ According to Shepard’s⁶¹, *United States v. Levin*, 874 F.3d 316, (1st Cir. 2017) has been followed or cited in 48 separate subsequent cases.⁶² However, questions remain regarding the scope and particularity of NIT warrants used in online investigations.

3.3.1 Rule 41 – Procedural or Substantial Changes?

The debate among scholars concerning Rule 41 (b) is centered on whether the changes to Rule 41 (b) were merely procedural or whether those changes substantially affected the Fourth Amendment’s guarantees against unreasonable search and seizure. There are strong opinions on both sides of the debate.

Hennessey (2017) contends that NITs are a necessary part of child exploitation investigations because “successful lawful hacking can lead to the identification of offenders and the rescue of child victims, . . . reduce the sense of security and comfort offenders feel in accessing and distributing child sexual abuse materials, . . . and should be

targeted at dismantling offender communities that proliferate on hidden services and other platforms.”⁶³ She further contends that the NIT Warrant was supported by probable cause because “the NIT was deployed only upon the completed crime of accessing the contraband image.”⁶⁴

Mercke (2018) likewise says the changes in Rule 41 (b) because they “were necessary in order to fix the glaring venue problems that cybercrimes caused for law enforcement and the courts . . . it merely allows magistrate judges to apply [Fourth Amendment] principles to an expanded digital realm.”⁶⁵ Hennessey similarly supports this position, stating that “we are now in the far more desirable situation of having a clear mechanism by which law enforcement can seek a warrant—subject to constitutional constraints—as opposed to the prior circumstances whereby law enforcement was unable to obtain a warrant even where it was clearly constitutionally permissible.”⁶⁶

Ohm (2017) contends that the changes to Rule 41 were principally valuable to conducting online investigations because “at least in police investigations of crimes occurring online, almost every new investigative lead comes bundled with probable cause. Unlike the physical world, the online world tends not to produce evidence that seems somewhat suspicious but not enough to establish probable cause, which means that we should no longer think of probable cause as the only

⁵⁹Id, 323

⁶⁰Id, 323.

⁶¹Shepard’s Citations is a citator used in United States legal research that provides a list of all the authorities citing a particular case, statute, or other legal authority.

⁶²Followed means to conform to or comply with the ruling being cited. Cited by makes reference to the previous ruling for the purpose of making a legal point in a finding.

⁶³Susan Hennessey, *The Elephant in the Room: Addressing Child Exploitation and Going Dark*, Aegis Paper Series 1701 (Stanford, CA: Hoover Institution, 2017), 12.

⁶⁴Hennessey, *The Elephant*, 19.

⁶⁵Bryan Mercke, “Dicing the Onion: An Analysis of Trans-Jurisdictional Warrants regarding Anonymous Cyber Crimes,” *University of Louisville Law Review* 56, no. 3 (2018): 458.

⁶⁶Hennessey, *The Elephant*, 16.

tool with which we protected ourselves from unfettered police investigations.”⁶⁷

Those observers that believe that the changes to Rule 41 were substantial in nature hold equally strong opinions. The Electronic Frontier Foundation (2016) contends that “the rules and proposals are supposed to be procedural and must not change substantive rights. But the amendment to Rule 41 isn’t procedural at all. It creates new avenues for government hacking that Congress never approved.”⁶⁸

Lerner (2016) contends that the changes to Rule 41 make it less likely that NIT warrant will be supported by probable cause because “it is unlikely that the government can demonstrate that the information seized from each person that visits a website throughout the surveillance period will be related to the investigation. While there may be some websites for which access alone may violate the law - such as a website that upon visitation disseminates child pornography to the user - the vast majority of websites will be frequented by legitimate users for whom probable cause does not exist.”⁶⁹

Russell (2017) argues that the changes to Rule 41 remove the procedures that safeguard against unreasonable search and seizure saying that “the substantial provisions of the Fourth Amendment serve as the only bar be-

tween residents of the Western District of Texas being hacked into by FBI agents in the Eastern District of Virginia based solely on a magistrate’s review.”⁷⁰

The Fourth Amendment requires that search warrants specify with particularity who is to be searched, where that search is to occur, and what may be seized as part of that search. Whether NIT warrants meet the particularity requirements for search warrants under the Fourth Amendment is another area of debate among scholars.

Referring to the FBI’s Playpen investigation that sparked the debate on NIT warrants, Lerner (2016) says that since “the government is unable to articulate either the location of the device to be searched or its IP address, there is reason to doubt the government’s ability to meet the particularity requirement.”⁷¹ He is also concerned that the lack of particularity makes NIT warrants akin to general warrants because they “need only specify that a given suspect has or will use the Internet to receive, store, or transmit evidence relevant to criminal activity.”⁷²

Rauschecker (2017) asserts that the changes to Rule 41 make it less likely that NIT warrants will lack particularity because “even if the government is able to demonstrate probable cause, it must no longer clearly identify the location of a computer to be searched, and it may use a single warrant to search thousands or even millions of computers.”⁷³

Some scholars contend that particularity requirements may be set aside when NITs are

⁶⁷Paul Ohm, "The Investigative Dynamics of the Use of Malware by Law Enforcement," *William Mary Bill of Rights Journal* 26, no. 2 (December 2017): 305.

⁶⁸Electronic Frontier Foundation, "With Rule 41, Little-Known Committee Proposes to Grant New Hacking Powers to the Government," *Electronic Frontier Foundation*, last modified April 30, 2016, accessed August 31, 2020, <https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government>.

⁶⁹Zack Lerner, "A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure," *Yale Journal of Law and Technology* 18 (2016): 48.

⁷⁰Zoe Russell, "First They Came for the Child Pornographers: The FBI’s International Search Warrant to Hack the Dark Web," *St. Mary’s Law Journal* 49, no. 1 (2017): 309.

⁷¹Lerner, "A Warrant," 49.

⁷²Lerner, 49.

⁷³Markus Rauschecker, "Rule 41 Amendments Provide for a Drastic Expansion of Government Authority to Conduct Computer Searches and Should Not Have Been Adopted by the Supreme Court," *Maryland Law Review* 76, no. 4 (2017): 1095.

deployed to investigate the sharing of child pornography via websites on the dark web. While society agrees that this type of crime deserves all that technology can bring to bear to defeat, some observers are concerned that NITs may be used to pursue websites that have nothing to do with child pornography.

Adams (2017) states that “regardless of the crime being investigated, courts must be cautious about the precedent set regarding how broadly the FBI can use NIT technology, [because] “this tactic could easily be utilized on more benign websites.”⁷⁴ Also questioning how broadly NITs are deployed, Aucoin (2018) concludes that “one person may easily draw a line for sex offenders, specifically child predators, while the next person may easily do the same for non-violent drug offenders. Whose line prevails here?”⁷⁵

The third area of comment from legal scholars concerns the changes that might be necessary to ensure that future searches conducted under NIT warrants comply with the Fourth Amendment. To avoid claims of dubious probable cause on searches of websites with mixed legal and illegal content, Merke (2018) states that “NITs should only be activated when the accessing computer navigates to pages on the website that contain illicit content.”⁷⁶ Lerner (2016) calls for more strict oversight, including “satisfying a preliminary showing that the location of the concealed device cannot reasonably be ascertained without an extraterritorial remote access search; requiring a thorough and technical descrip-

tion of both the search tool’s installation process and location collection method; and mandating the implementation and description of minimization and accountability measures to limit harm.”⁷⁷

Other observers argue that the deployment of NITs should be restricted to known websites hosting illicit content. In those instances, Adams (2017) says that the government “should reasonably limit the scope and probability of ensnaring those stumbling upon the site by planting the NIT code, not on the home page, but further within the website so that an individual’s happenstance encounter with the site does not trigger the search.”⁷⁸

Calling for more supervisory oversight and review, Daskal (2016) argues that such reviews “should demand rigorous and periodic security reviews by both internal and independent experts of the tools being employed.”⁷⁹ Ohm (2017) contends that legislation is needed, saying that “Congress could enact a new law, for example, perhaps modeled on the Wiretap Act - necessity, internal review, and predicate crimes, that required more than the baseline requirements of probable cause and review by a detached and neutral magistrate before the police could be granted a warrant to deploy [NITs].”⁸⁰

Finally, some claim that the potential abuses of power are too dangerous for NITs to be deployed at all. As one observer noted, “Courts have said that dangerous tools used to effectuate otherwise lawful searches — tools like flashbang grenades and battering rams — can be unreasonable under the

⁷⁴Devin M. Adams, "The 2016 Amendments to Criminal Rule 41: National Search Warrants to Seize Cyberspace, Particularly Speaking," *University of Richmond Law Review* 51, no. 3 (March 2017): 762.

⁷⁵Kaleigh E. Aucoin, "The Spider's Parlor: Government Malware on the Dark Web," *Hastings Law Journal* 69, no. 5 (June 2018): 1469.

⁷⁶Bryan Mercke, "Dicing the Onion: An Analysis of Trans-Jurisdictional Warrants regarding Anonymous Cyber Crimes," *University of Louisville Law Review* 56, no. 3 (2018): 460.

⁷⁷Lerner, "A Warrant," 62-63.

⁷⁸Adams, "The 2016," 767.

⁷⁹Jennifer Daskal, "Rule 41 Has Been Updated: What's Needed Next," *Just Security* (blog), entry posted December 5, 2016, accessed October 7, 2020, <https://www.justsecurity.org/35136/rule-41-updated-needed/>.

⁸⁰Ohm, "The Investigative," 329.

Fourth Amendment. Government malware is another such tool. Some investigative techniques are just too dangerous to use.”⁸¹ To date, there has been no legislative debate as to whether the change to Rule 41 was procedural (i.e., what a magistrate can authorize and under what conditions), or whether it was substantial (i.e., a change to the Fourth Amendment that allows for the conditional use of general warrants).

3.4 Geo-Fence Warrants

The Fourth Amendment guarantees the right of citizens to be secure in their persons from all unreasonable searches and seizures. In *Katz v. United States*, 389 U.S. 347 (1967), the United States Supreme Court redefined what constitutes a search and seizure by instituting the *Katz* test for the reasonable expectation of privacy. The two-part test states that “first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as “reasonable.””⁸²

The introduction of new technologies continues to pose challenges for the courts to determine what constitutes a search and seizure and how to apply the *Katz* test for a reasonable expectation of privacy. The use of geo-location by law enforcement in tracking potential suspects’ movements is one of those technologies challenging the courts.

In *Carpenter v. United States*, 138 S. Ct. 2206 (June 22, 2018), the Supreme Court set a precedent with regard to geo-fence warrants. Timothy Carpenter was arrested along with three other men in April 2011 after a lengthy investigation by Detroit police department into a string of unsolved robberies at local

T-Mobile and Radio Shack stores. The four men were subsequently charged with aiding and abetting a *Hobbs Act* robbery and various related weapons charges.⁸³ One of the men arrested confessed to the robberies and provided detectives with his cell phone number and the cell phone numbers of others involved in the robberies.

From this information, detectives applied for a geo-fence warrant to obtain transactional information from several wireless carriers for “all subscriber information, toll records and call detail records including listed and unlisted numbers dialed or otherwise transmitted to and from [the] target telephones from December 1, 2010, to present, as well as cell site information for the target telephones at call origination and at call termination for incoming and outgoing calls.”⁸⁴ Along with his co-defendants, Carpenter was ultimately charged with six *Hobbs Act* violations.

At trial, the government introduced evidence that demonstrated “that each man used his cellphone within a half-mile to two miles of several robberies during the times the robberies occurred.”⁸⁵ The defendants challenged the collection of the cell service provider’s records from the geo-fence warrant, arguing that the collection of those records constituted a warrantless search, violating the Fourth Amendment. The district court denied the motion, and Carpenter was convicted and sentenced to serve 1,395 months.

Carpenter then appealed to the United States Court of Appeals for the Sixth Circuit, challenging the district court’s denial of their motion to suppress the cell service provider records. Those records included cell-site lo-

⁸¹Plus Media Solutions, "Challenging Government Hacking: What’s at Stake," US Official News (London, UK), November 2, 2017.

⁸²*Katz v. United States*, 389 S. Ct. 347, 361 (Dec. 18, 1967), (Harlan concurring).

⁸³*The Hobbs Act* (1946) prohibits actual or attempted robbery or extortion affecting interstate or foreign commerce in any way or degree.

⁸⁴*United States v. Carpenter*, 819 F.3d 880, 884 (6th Cir. 2013).

⁸⁵*Id.*, 883.

cation information, covering 127 consecutive days of records.

In denying Carpenter’s appeal, the Sixth Circuit ruled that “government’s collection of business records containing cell-site data was not a search under the Fourth Amendment, and suppression of evidence was not among the remedies available for alleged violations of the Stored Communications Act.”⁸⁶⁸⁷

In his concurring opinion, however, Justice Stranch sounded a warning when he wrote: “I am also concerned about the applicability of a test that appears to admit to no limitation on the quantity of records or the length of time for which such records may be compelled. I conclude that our precedent suggests the need to develop a new test to determine when a warrant may be necessary under these or comparable circumstances.”⁸⁸

The stage was set for Carpenter to take his appeal to the Supreme Court. On November 29, 2017, the court heard arguments from the plaintiff and the government’s attorneys. Justice Roberts described the stakes at hand, saying, “this case presents the question whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user’s past movements.”⁸⁹

On June 22, 2018, the Supreme Court ruled in favor of Carpenter, saying that “government’s acquisition from wireless carriers of defendant’s historical cell-site location information (CSLI) was a search under the Fourth Amendment.”⁹⁰ Going further, the

court ruled that when “the government accessed defendant’s CSLI, it invaded his reasonable expectation of privacy in the whole of his physical movements, and the fact that the government obtained the information from a third party did not overcome defendant’s claim to Fourth Amendment protection.”⁹¹

Finally, the court determined that a search warrant was required for the government to obtain cell-site location information (CSLI). In making their ruling, the court clarified Fourth Amendment protections and the reasonable expectation of privacy for the digital age. In so doing, the court also recognized that their ruling was narrow – that there may be exigent circumstances that demand obtaining CSLI in the absence of a search warrant. What those circumstances may have yet to be fully determined.

Since the Supreme Court ruling in *Carpenter*, the Ninth Circuit ruled that that “CSLI acquired *pre-Carpenter* is admissible — so long as the Government satisfied the SCA’s then-lawful requirements — under Krull’s good-faith exception.”⁹² This would appear to make moot any future appeals that come before the U.S. Courts of Appeal on matters related to *pre-Carpenter* CSLI data.

3.4.1 Search and Seizure and the Reasonable Expectation of Privacy

The debate over law enforcement’s use of geo-fence warrants to investigate crimes and identify suspects is concerned with the following questions:

- Are geo-fence search warrants particularized to the extent that they are not general warrants?

⁸⁶Id, 890.

⁸⁷The search warrant for the cell site provider records was obtained under provisions of the Stored Communications Act (SCA, codified at 18 U.S.C. Chapter 121 §§ 2701–2712).

⁸⁸*United States v. Carpenter*, 819 F.3d 880, 896 (Stranch concurring).

⁸⁹*Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018).

⁹⁰Id, 2220.

⁹¹Id, 2220.

⁹²*United States v. Korte*, 918 F.3d 750, 759 (9th Cir. 2019), citing *Illinois v. Krull*, 480 U.S. 340, 107 S. Ct. 1160 (1987).

- Should a search warrant supported by probable cause be required for any geo-fence search warrant?
- Is CSLI data reliable? If not, should it be admitted as evidence?
- Finally, should law enforcement agencies skirt the Carpenter ruling by buying CSLI data from private companies?

Citing concerns about the scope of geo-fence warrants, in 2019, the Electronic Frontier Foundation (EFF) said that “most of the information provided to law enforcement in response to a geo-fence warrant does not pertain to individuals suspected of the crime . . . search results are both over and under inclusive . . . and the user’s Google identifies in response to a geo-fence warrant may not even be within the geographic area defined by the warrant (and therefore are outside the scope of the warrant).”⁹³ Also concerned with the particularity of these warrants, the EFF stated that they “lack particularity because they don’t properly and specifically describe an account or a person’s data to be seized. They result in overbroad searches that can ensnare countless people with no connection to the crime.”⁹⁴

Geo-fence warrants obtained under the *Stored Communications Act* do not require notification to the targets of electronic of surveillance. Bloch-Wehba (2020) contends that “secrecy threatens to undermine the effectiveness of checks on law enforcement because the public lacks any real opportunity

⁹³Jennifer Lynch, "EFF Files Amicus Brief Arguing Geofence Warrants Violate the Fourth Amendment," Electronic Frontier Foundation, last modified July 2, 2020, accessed July 31, 2020, <https://www.eff.org/deeplinks/2020/07/eff-files-amicus-brief-arguing-geofence-warrants-violate-fourth-amendment>.

⁹⁴Lynch, "EFF Files," Electronic Frontier Foundation.

to mobilize against abusive practices.”⁹⁵ According to her, public scrutiny of geo-fence warrants is necessary as a response to “warrantless surveillance at scale.”⁹⁶

Priester (2019) adds to the discussion of warrantless seizure at scale, observing that “data-driven surveillance allows the Government to gather vastly greater quantities of information about a person than has ever been possible before . . . and data-driven surveillance also provides the Government with information of a very different qualitative nature than has ever existed previously.”⁹⁷

The lack of particularity in geo-fence warrants concerns scholars like Elm (2020), who observes that “innocent bystanders may have their personal information sucked up by police in wholesale ways that wouldn’t have happened before the ubiquity of internet connected smartphones.”⁹⁸ Because of this, Elm says that police should restrict the use of geo-fence to more serious, violent crimes and clearly detail the probable cause upon which their search warrant is based. Elm argues that even in these instances “the Fourth Amendment prohibits police from going door-to-door to search innocent households for the suspect, so the ‘general warrant’ and the Particularity Clause ultimately may put an end to these warrants.”⁹⁹

Finally, some scholars contend that using historical cell site location information (CSLI) is unreliable and should be ruled as inadmis-

⁹⁵Hannah Bloch-Wehba, "Transparency after Carpenter," Washburn Law Journal 59, no. 1 (Winter 2020): 29.

⁹⁶Bloch-Wehba, "Transparency after," 29.

⁹⁷Benjamin J. Priester, "A Warrant Requirement Resurgence: The Fourth Amendment in the Roberts Court," St. John’s Law Review 93, no. 1 (2019): 127.

⁹⁸Donna Lee Elm, "Geofence Warrants: Challenging Digital Dragnets," Criminal Justice 35, no. 2 (Summer 2020): 10.

⁹⁹Elm, "Geofence Warrants," 13.

sible under *Rule 702* of the Federal Rules of Evidence (the Daubert Test). Kirkham (2019) observes that the coverage maps created by service provider “were not created for location-tracking purposes, but for internal business decisions of the cellular company.”¹⁰⁰ He says that although service providers have business reasons for collecting CSLI, “none of those reasons involve historical location tracking of a cell phone. Only law enforcement employs [CLSI] for that purpose.”¹⁰¹ An additional problem with geo-fence warrant is a loophole in *Carpenter* that has led some law enforcement agencies to exploit by buying location data from private companies rather than applying for a warrant to search cell phone carrier records as required by *Carpenter*. According to Cushing (2020), “federal agencies are going to want this loophole kept open. Since it’s unlikely the government is informing courts about this use of data, there have been no courtroom challenges of this practice, leaving the feds free to operate in this precedent-free void.”¹⁰² He concludes by saying that although federal agencies “are playing to the edges of the Fourth Amendment right now and it might come back to hurt them.”¹⁰³

¹⁰⁰Thomas J. Kirkham, "Rejecting Historical Cell Site Location Information as Unreliable under Daubert and Rule 702," *University of Toledo Law Review* 50, no. 2 (Winter 2019): 371.

¹⁰¹Kirkham, "Rejecting Historical," 372.

¹⁰²Tim Cushing, "Secret Service Latest to Use Data Brokers to Dodge Warrant Requirements for Cell Site Location Data," *Techdirt* (blog), entry posted August 24, 2020, accessed September 8, 2020, <https://www.techdirt.com/articles/20200820/13395145155/secret-service-latest-to-use-data-brokers-to-dodge-warrant-requirements-cell-site-location-data.shtml>.

¹⁰³Cushing, "Secret Service," *Techdirt* (blog).

3.5 Appeals Related to the Legal Landscape

Referencing the discussion on the legal landscape, we see the following results. Of the 112 cases included in this study, fifty-seven (50.89%) were related to the areas of jurisprudence discussed in the first section of this study. Five were related to border searches, one was related to compelled decryption, twenty-eight were related to geo-fence warrants, and twenty-three were related to NIT warrants. There are myriad reasons for this.

For compelled decryption, it is likely that these types of appeals will make their way to the U.S. Courts of Appeal but are currently in the State court system or are in the federal district court system. In some instances, appeals were made but dismissed because the defendant had no standing to appeal (i.e., the objection was not made or preserved at trial). With regard to border searches, and compelled decryption, it is possible that certain defendants are waiting for the Supreme Court to make a decision on those areas of jurisprudence before submitting their appeals.

Of the appeals that were related to the areas of jurisprudence discussed, only one resulted in a decision that favored the defendant. The next section highlights that appeal.

3.5.1 *United States v. Cano*, 934 F.3d 1002 (9th Cir. 2019)

On July 25, 2016, Miguel Cano was arrested shortly after arriving at the San Ysidro Port of Entry from Tijuana. Cano’s vehicle was diverted to a secondary inspection following a random Customs and Border Protection (CBP) agency computer referral. During this secondary inspection, CBP dogs detected the presence of narcotics in the vehicle’s spare tire. Upon inspection, CBP agents found over 30 pounds of cocaine inside fourteen vacuum-sealed packages.

Cano was subsequently arrested on suspicion of drug trafficking, and his cell phone was seized. After a brief manual inspection of the cell phone, CBP agents conducted an invasive secondary search. This search included using the cell phone forensics tool, Cellebrite, to conduct a logical download of the phone's contents. The logical download yielded text messages, contacts, call logs, and any media contained on the phone.

Miguel Cano was later indicted for importing cocaine. During his evidentiary hearing, Cano moved to suppress the evidence obtained during the initial manual search and the subsequent invasive search conducted using Cellebrite. The court denied the motion to suppress, ruling that both the initial and subsequent searches were subject to the border exception for searches.

After a mistrial, Cano was convicted following his second trial for importing cocaine. On April 27, 2017, Cano was committed to the custody of the U.S. Bureau of Prisons for a term of 54 months. Miguel Cano appealed his conviction to the 9th Circuit Court of Appeals.

In considering Cano's appeal, the court addressed the following issues: 1) whether any warrantless search of a cell phone falls outside the scope of the border search exception; 2) if the search is within the scope of the border search exception, whether a warrantless cell phone search is so intrusive that it requires probable cause; 3) even if cell phones are generally subject to search at the border, whether the manual and forensic searches of Cano's cell phone exceeded the scope of the border search; and 4) if the search was conducted in good faith, whether the evidence should nevertheless be admissible¹⁰⁴.

The panel from the 9th Circuit determined that cell phones are subject to search at the

¹⁰⁴*United States v. Cano*, 934 F.3d 1002, 1012 (9th Cir. 2019).

border, declaring that "manual searches of cell phones at the border are reasonable without individualized suspicion, whereas the forensic examination of a cell phone requires a showing of reasonable suspicion."¹⁰⁵ Therefore, Cano's cell phone was subject to a search.

In considering whether a warrantless search of a cell phone is so intrusive as to require probable cause, the panel held that "that manual searches of cell phones at the border are reasonable without individualized suspicion, whereas the forensic examination of a cell phone requires a showing of reasonable suspicion."¹⁰⁶

In determining whether the manual and forensic searches of Cano's cell phone exceeded the scope of the border search, the panel concluded that "that border officials may conduct a forensic cell phone search only when they reasonably suspect that the cell phone to be searched itself contains contraband."¹⁰⁷

Concluding that CBP agents did not have reasonable suspicion, then "the Cellebrite search of Cano's cell phone qualifies as a forensic search, the entire search was unreasonable under the Fourth Amendment."¹⁰⁸ In their final word on the matter, the court held that "the border search exception did not authorize the agents to conduct a warrantless forensic search of Cano's phone, and evidence obtained through a forensic search should be suppressed."¹⁰⁹

The panel from the 9th Circuit determined that the good faith exception to the exclusionary rule did not apply. Referring to their ruling in *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013), the panel said that "Cotterman was a search for contraband that the government has a right to seize at

¹⁰⁵*Id.*, 1014.

¹⁰⁶*Id.*, 1018.

¹⁰⁷*Id.*, 1020.

¹⁰⁸*Id.*, 1021.

¹⁰⁹*Id.*, 1021.

the border. Here, the officials' search was objectively tied only to proving their case against Cano and finding evidence of future crimes. Searching for evidence and searching for contraband is not the same thing."¹¹⁰

The panel from the 9th Circuit reversed the District Court's denying Cano's motion for suppression and vacated his conviction. There has been no subsequent court action related to Miguel Cano.

4. LIMITATIONS

This study examined appeals of in criminal cases before the United States Courts of Appeal, focusing on significant areas of jurisprudence affecting decisions made in appeals involving some aspect of digital evidence. The author is a program manager with the National Institute of Justice (NIJ), an agency of the U.S. Department of Justice's Office of Justice Programs. Part of NIJ's mission is to provide objective and independent knowledge and tools to inform the decision-making of the criminal and juvenile justice communities to reduce crime and advance justice. As such civil matters were not considered for inclusion in this study. It may be worthwhile for future researchers to examine how digital evidence fares in civil matters before the U.S. Courts of Appeal.

Additionally, the appeals included in this study resulted from searches executed within Lexus Advance. Accordingly, examining the potential bias of the jurists or deciphering the mind of jurists was outside the scope of the current study.

Finally, the search terms used may have missed some appeals involving digital evidence. However, the author is confident that the issues raised herein were adequately represented by the cases cited.

¹¹⁰Id., 1022.

5. CONCLUSIONS

In the previous study's conclusions, it was suggested that digital evidence from wearable Internet of Things devices would make its way into the United States Courts of Appeal. It should be noted that no cases came before the United States Courts of Appeal that involved digital evidence derived from the Internet of Things between 2016 and 2020. However, that may soon change.

In 2016, evidence from a Fitbit was used to exonerate a suspect in the murder of his wife in Wisconsin ¹¹¹. In that same case, location evidence from a Google Dashboard application helped convict the perpetrator. In 2018, digital evidence from a pacemaker helped detectives charge a suspect accused of committing arson by setting his own dwelling ablaze ¹¹².

While the Internet of Things may well be the coming storm, the digital evidence associated with criminal cases before the United States Courts of Appeal from 2016 to 2020 came from an assortment of computers, laptops, cell phones, and GPS-enabled devices.

The areas of jurisprudence discussed in section three have profound implications for decisions made in appeals of criminal cases before the United States Courts of Appeal. Those decisions affect how police conduct investigations, what evidence a prosecutor may choose to introduce at trial, and how likely that evidence will be considered admissible in court.

Citizens will still be subject to searches at the nation's borders. Investigators will still need to unlock digital devices to uncover potential evidence. Law enforcement will still need to deploy unique methods to catch criminals hiding behind the dark web's anonymity. Furthermore, finally, investigators will still

¹¹¹State v. Burch, CN: 2016CF001309 (WI, 2018)

¹¹²State v Ross Compton, Case No. CR 2016-12-1826 (OH, 2017).

need to determine the whereabouts of potential suspects in criminal investigations. How these actions are all accomplished will spark continued debate among scholars and ensure a steady stream of decisions handed down in the U.S. Courts of Appeal that may be definitive, occasionally contradictory, and always noteworthy.

6. TABLES

Table 1 - Comparison of Offenses. 4
 Table 2 - Comparison of evidence types. 5

7. TABLE OF AUTHORITIES

CASES

Carpenter v. United States, 138 S. Ct. 2206
 (June 22, 2018) ————— 16
Katz v. United States, 389 U.S. 347 (1967)
 ————— 16
re Search of a Residence in Oakland, 354
 F. Supp. 3d 1010 (N.D. Cal. 2019) —p10
Riley v. California, 134 S. Ct. 2473 (2014)
 ————— 6
United States v. Cano, 934 F. 3rd 1002
 (9th Cir. 2019) ————— 20
United States v. Cotterman, 709 F.3d 952
 (9th Cir. 2013) ————— 21
*United States v. Doe (In re Grand Jury
 Subpoena Duces Tecum)*, 670 F.3d 1335
 (11th Cir. 2012) ————— 9
United States v. Krueger, 809 F.3d 1109
 (10th Cir. 2015) ————— 12
United States v. Leon, 468 U.S. 897
 (1984) ————— 11
United States v. Levin, 874 F.3d 316,
 (1st Cir. 2017) ————— 12