No. 10-1011

In The Supreme Court of the United States

HECTOR ESCATON,

Petitioner

v.

UNITED STATES OF AMERICA,

Respondent

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FOURTEENTH CIRCUIT

BRIEF FOR THE PETITIONER

TEAM 12

Counsel for the Petitioner

TABLE OF CONTENTS

TABLE OF AUTHORITIES

UNITED STATES SUPREME COURT CASES:

UNITED STATES COURT OF APPEALS CASES:

UNITED STATES DISTRICT COURT CASES:

STATE SUPREME COURT CASES:

INTERNATIONAL CASES:

CONSTITUTION, STATUTES/CODES AND DIRECTIVES USED:

OTHER AUTHORITIES

QUESTIONS PRESENTED

1. Whether the Fourth Amendment requires that the government officers must have reasonable suspicion before conducting forensic searches of electronic devices at an international border?
2. Whether the government's acquisitions pursuant to 18 U.S.C. § 2703(d) of three days of cell-site location information, one-hundred cumulative hours of cell-site location information over two weeks, and cell-site location information collected from cell tower dumps violate the Fourth Amendment of an individual in light of this Court's limitation on the use of cell-site location information in *Carpenter v. USA,* 138 S. Ct. 2206 (2018)

OPINION BELOW

The United States Court of Appeals of the 14th Circuit, upheld the decision in the Trial Court and denied the Petitioner's motion to suppress evidence obtained from the forensic search of his electronic devices at the border, and the cell site location information obtained that was later used to convict him of bank fraud, 18 U.S.C. § 1344, conspiracy to commit bank fraud, §1349, and aggravated identity theft, 18 U.S.C. § 1028A. The decision below is reported as: *Escaton v. United States*, 1001 F.3d 1341 (14th Cir. 2021)

CONSTITUTIONAL PROVISIONS AND RULES

The Fourth Amendment to the Constitution of the United States reads as:

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

[U.S. CONST. amend. IV.]

INTRODUCTION

Hector Escaton (*hereinafter* 'Petitioner'/'Escaton') has been charged with Bank Fraud (18 U.S.C. § 1344), Conspiracy to Commit Bank Fraud (18 U.S.C. § 1349), and Aggravated Identity Theft (18 U.S.C. § 1028A). This is an appeal challenging the decision made by the District Court, subsequently affirmed by the 14th Circuit Court of Appeals which denied the Petitioner's Fourth Amendment rights and his motion to suppress the evidence pertaining to: (i) the forensic search at the border and, (ii) cell-site data requested from Delos Wireless.

The forensic search of the Petitioner's electronic devices at the border infringed upon his right to privacy and thereby violated his Fourth Amendment rights. Not distinguishing between electronic devices (specifically data) and other possessions at the border, leads to a perverse conclusion of Fourth Amendment jurisprudence. Essentially allowing agents situated at the border to conduct an intrusive search into one's life. A search of such a nature can be termed as a particularly offensive one, or a search which goes against one's personal dignity and thereby be termed as non-routine requiring reasonable suspicion for the same. The Court's reliance on 'national security' as only an inbound threat, undermines the fact that devices of such nature pose a threat irrespective of geographical positioning. Lastly, the Court fails to take into consideration that there was an act of circumvention by the CBP Officer at the border. By handing over the device to the ICE officer, there was no compliance with the CBP Directive of 2018, as the ICE officer's powers are derived from ICE's 2009 policy. In such a case, the failure to conduct a search on mere reasonable suspicion, a standard lower than probable cause, should lead to the operation of the exclusionary rule, thereby suppressing such evidence procured as a result of an illegal search.

The FBI's requests for the Cell Site Location Information (*hereinafter* 'CSLI') was clearly violative of the Petitioner's Fourth Amendment right to be secure against unreasonable searches. Escaton had a reasonable expectation of privacy in the whole of his physical movements, regardless of the duration of surveillance. Further, merely because the Petitioner was operating on public thoroughfares does not mean that he did not have a bearing on his right to be secure against Government intrusions as to his person and privacy. Even on applying the doctrine of common-law trespass, it is clear that the Petitioner sought to maintain his location information as private, and that he had a legitimate proprietary claim as to his digital data. Finally, the data obtained by tower dumps is indicative of the arbitrary tool it may turn into for the purposes of law enforcement, where it permits a fishing expedition. The failure to procure a warrant for a search of such an intrusive nature should result in the application of the exclusionary rule, thereby suppressing such evidence procured as a result of an illegal search.

STATEMENT OF THE CASE

On September 25, 2019, Hector Escaton was stopped at the United States Border Checkpoint at West Texas, of where he was a citizen and resident (R. at 2). CBP Officer, Ashley Stubbs, upon conducting a preliminary search, found Escaton's iPhone, laptop, three external hard drives, and four USB devices. Officer Stubbs then proceeded to manually check the devices, and detained all of them apart from the iPhone (R. at 3). While trying to gain access, it was clear that the laptop in itself was not password protected, only some folders were; and the USB devices had inaccessible content when plugged in. (R. at 3). Without any reasonable suspicion (R. at 2, 6), the devices were delivered to ICE Agent, Theresa Cullen, at the border checkpoint, who proceeded to use

forensic software to copy and scan the devices. The results of the examination revealed documents containing individual's bank account numbers and pins; and the USB devices bore traces of malware (R. at 3).

The findings were sent to the FBI, who were investigating the 'ATM Skimming' of Mariposa Bank ATMs in Escalante and Sweetwater. Agent Catherine Hale from the FBI examined the results of the forensic search and the ATM skimming reports which indicated that 'several methods' had been used to steal information and cash from the ATMs. However, only one these methods indicated at a mechanism of skimming with malware installed through a USB port from Sweetwater ATMs. (R. at 4). Further, as per the forensic search it was revealed that the malware found on Escaton's USB device was only 'similar' to the malware used at two Mariposa Sweetwater ATMs (R. at 3, 4, 5). No information was recovered from the Escalante ATMs, as there was a loss of stored data due to an internal-testing malfunction (R. at 4).

Agent Hale then proceeded to acquire three tower dumps for a total of three hours of location cell-points from three Sweetwater ATMs under 18 U.S.C. § 2703(d) (1986) of the Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2006) [*hereinafter*, 'SCA'], which requires 'specific and articulable' facts, less than probable cause. (R. at 4 and 10). This was provided in the form of an affidavit. Hale. Aff. ¶ 3. Based on the similarity of malware and fact that one of the phone numbers obtained from the three tower dumps matched Escaton's (R. at 5), Agent Hale along with Attorney Hughes obtained Escaton's CSLI from his service provider, Delos Wireless, for three days [Three-day Records] under the SCA. Further, in order to try placing Escaton at Escalante, they once again obtained CSLI for his as well as another individual's (whose name, Delores, and number were found on the basis of the preliminary search by Officer Stubbs). This

second request spanned for 10 days, but covered only weekdays during working hours (8:00AM-6:00PM MDT) [Weekday Records].

Both of these requests, along with the tower dump requests, were warrantless, and merely on the basis of 'specific and articulable facts' to show that the records would be relevant to the ATM skimming of Mariposa Bank. Hale. Aff. ¶ 3. As a consequence, the Three-day Records placed Escaton near Sweetwater, which is densely populated with very accurate cell-site location information. While the Weekday Records of Escalante, a suburban town with sparse cell towers, Hale. Aff. ¶ 11, 12, placed Delores in the vicinity; and the same cell-site tower recorded both, Delores and Escaton's number, allegedly placing him with her (R. at 5). Based on the CSLI records obtained from Delos Wireless by Attorney Hughes and Agent Hale, Escaton was convicted. (R. at 6).

Escaton was charged with Bank Fraud, 18 U.S.C § 1344, Conspiracy to Commit Bank Fraud 18 U.S.C § 1349, and Aggravated Identity Theft, 18 U.S.C § 1344. (R. at 6). Escaton sought to suppress two records of evidence at trial: (i) the results of the forensic search of his digital devices which was obtained by the law enforcement without reasonable suspicion (R. at 6); and (ii) the cell-site data obtained from Delos wireless, under the SCA as per 18 U.S.C. § 2703(d). (R. at 6, 10). The District Court denied the motion (R. at 6), and Escaton appealed after being convicted by a jury. *Id*. A divided panel of Judges at the Fourteenth Circuit upheld the District Court's ruling, finding that **(a)** No reasonable suspicion is necessary for a forensic examination of electronics at the border (R. at 6), and **(b)** The historical CSLI obtained by law enforcement did not violate the Petitioner's Fourth Amendment rights. (R. at 10). This appeal followed.

ARGUMENTS

I. THE PETITIONER MAINTAINS A DEGREE OF PRIVACY, EVEN AT THE BORDER, WHICH WOULD REQUIRE A STANDARD OF REASONABLE SUSPICION BEFORE A FORENSIC SEARCH OF ANY OF HIS ELECTRONIC DEVICES CAN TAKE PLACE.

A. COURTS MUST DIFFERENTIATE BETWEEN PHYSICAL OBJECTS AND ELECTRONIC DEVICES AT THE BORDER, WHERE NON-ROUTINE BORDER SEARCHES MUST FOLLOW THE ANALYSIS SET FORTH IN *RILEY,* MANDATING REASONABLE SUSPICION.

The essence of technology creates a unique distinction between physical objects and electronic devices which the courts must recognize in order to substantially identify the existence of one's privacy concerns at the border. The degree of intrusiveness caused by forensic searches of electronic devices at the borders are not only harmful, but are equally offensive. They have the potential to look beyond the physical realm and into the intangible realm of data which is not present at the border itself. The courts need to take into consideration the analysis set forth in *United States v. Ramsey*, 431 U.S. 606 (1977), and other precedents to adhere to the same, in terms of requiring reasonable suspicion before a forensic search of electronic devices.

i. The application set forth in *Touset* is unsustainable as the courts did not differentiate between physical property and electronic devices at the borders.

In this era of digital advancement, it is imperative to differentiate between physical properties and electronics. The analysis set forth in *Riley v. California*, 134 S.Ct. 2473 (2014), and *United States v. Brima Wurie*, 728 F.3d 1 (1st Circ. 2013), create distinct categorizations of cell phones on one hand, and physical objects on the other. The direct application of *United States v. Touset,* 890 F.3d 1227 (11th Circ .2018), without differentiating between physical properties and electronics at the border leads to a risky precedent being set which would thereby give broad powers to the U.S Customs and Border Protection [*hereinafter* 'CBP'] and Immigrations and

Customs Enforcement [*hereinafter, '*ICE'] to infringe on one's dignity and privacy without having any reasonable suspicion to do so.

While differentiating a gas tank to a cell phone, one must keep in mind the "uniquely sensitive nature of data on electronic devices" *United States v. Cotterman*, 709 F.3d 952, 966 (9th Cir. 2013), which essentially renders an *"*exploratory search more intrusive than other forms of property." *Id.* at 966. In *Cotterman,* there was an emphasis on the fundamental difference between border searches of physical belongings, as against those of a forensic search of a device. The wealth of data on an electronic device is comparable to a "warehouse full of information," *Cotterman*, 709 F.3d 952 at 964, which would have a greater intrusion on the personal life of a traveler than the physical objects he could possibly carry.

As the Supreme Court explained in *Riley*, 134 S.Ct. at 2489, cell phones are "minicomputers*"* carrying an immensely diverse amount of data. It would be an extenuating argument to compare such powerful devices to material objects at the border which a person could physically carry. Thus highlighting the qualitative difference of such data from actual physical goods, stating that "little else justifies lumping them together." *Id.* at 2488.

Similarly, travelers are known to be aware of what tangible material they carry with them at the borders, however a forensic search of an electronic device can potentially access deleted files which the traveler never intended to carry, or simply wasn't aware of. As noted in *United States v. Flyer,* 633 F.3d 911 (9th Cir. 2011), "unallocated space (on a hard drive) contains deleted data (...) [which] cannot be seen or accessed by the user without the use of forensic software." *Id.* at 918. This form of an intrusive search can thus discover unintended private data which the traveler perhaps never wanted to cross the border with.

Similarly, cloud data can "appear as a seamless part of the digital device when presented at the border," *Cotterman*, 709 F.3d at 965, thereby showing the ubiquitous nature of such devices. This can cause the border agents to be unable to tell the difference between the information stored locally, or being extracted from the cloud. Thus allowing a search for information which is not physically present with the traveler at the border itself. *Riley* 134 S.Ct. at 2491.

Furthermore, comparing the same with a physical object would give the border patrol officers unrestricted access to intricate and private data under the justification of it being the same as a physical object. Thus, the Petitioner humbly submits that the analysis set forth in *Touset,* 890 F. 3d 1227, does not take into consideration the underlying difference between physical objects and electronic devices at a border, which cannot be applied *simpliciter*.

ii. <u>Considering the volatile nature of data, the Court should deem forensic searches of electronic devices as 'non-routine' and consider them contravening personal dignity.</u>

In terms of searches being claimed as non-routine requiring reasonable suspicion, there has been some ambiguity regarding the line being drawn with respect to the amount of intrusiveness which could be deemed as warranting reasonable suspicion. However, in the past, intrusive searches have been defined *"*in terms of the indignity that will be suffered by the person being searched," *United States v. Vega-Barvo*, 729 F.2d 1341, 1345 (11th Cir. 1984), or which were done in a "particular offensive manner," *Ramsey*, 431 U.S. at 618 n.13, as non-routine, thereby requiring a reasonable suspicion.

We humbly submit that *Touset* failed to recognize that the degree of intrusiveness with regard to a 'digital strip search' at the border is significantly similar to a body cavity search – the jurisprudence for which requires a degree of reasonable suspicion. *Montoya,* 473 U.S. at 542, 559. Consequentially, a forensic search of a device requires reasonable suspicion, as it bears an

inherent distinction from a physical object [**I A(i)**]. Primarily because **(a)** there exists a great deal of 'intrusion', and **(b)** such an intrusion impacts an individual's dignity.

Electronic devices have a similar bearing to the memories of an individual, which is a private affair. In this modern age the replication of feeling or a sensation can be stored in an electronic device, as they "function as an extension of our own memory." *United States v. Arnold*, 454 F. Supp. 2d 999**,** 1000-01 **(**C.D**.** Cal. 2006), rev'd*, 533* F**.**3d 1003 (9th Cir. 2008). The Court in *Arnold* claimed that "government intrusions into the mind – specifically those that would cause fear or apprehension (…) are no less deserving [of] the Fourth Amendment." *Id.* Although it was reversed on appeal, the analysis of *Arnold* is useful in realizing the significance in the level of invasiveness and dignity harmed with government intrusions. Likewise, as cellphones and digital devices have an integral role to play, similar to painting a "detailed, intimate, individual portrait of the user," Eunice Park, *The Elephant in the Room: What is a nonroutine Border Search, anyway: Digital Device Searchers Post-Riley,* 44 Hastings Const.L.Q. 277, 300 (2019), they deserve Fourth Amendment protection.

Similarly, 'indignity' is defined as "something that causes a loss of respect for someone or for yourself," *Indignity Definition*, DICTIONARY.CAMBRIDGE.ORG, https://dictionary.cambridge.org/dictionary/english/indignity (last visited Feb. 8, 2019), thereby showing the relative nature of the word. It cannot be defined in mechanical terms and applied only to bodily features. Due to their immense storage capacity, digital devices can record and show intimate information such as – every book an individual has read, their medical data, details about their sexual relations, and much more. In fact, digital devices can be perceived as "an important feature of human

anatomy." *Riley* 134 S.Ct. at 2484. Hence, it is imperative that electronic devices are understood as distinct from other physical objects, based on this fragility and wealth of information.

ICE's 2009 Directive, *see* U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, BORDER SEARCHES OF ELECTRONIC DEVICES, DIRECTIVE NO. 7-6.1 § 6.1 (AUG. 18, 2009), http://www.dhs.gov/sites/default/files/publications/7-6.1%20directive.pdf. [*hereinafter*, 'ICE 2009 Directive'], creates a broader invasion into one's privacy by allowing ICE agents to access the information stored in the cloud which is not on the devices itself. The level of intrusiveness is patently arbitrary, as the officer can access information such as "a traveler's home via live video feeds provided by home security apps." Brief for Petitioner as Amicus Curiae at 17, United States of America v. Hamza Kolsuz, 890 F.3d 133 (4th Circ.2018) (No. 16-4687, 24-1). Further, detailed information is available concerning even "a traveler's financial life with (…) apps that link to bank, credit card, and retirement accounts." *Id.* at 16. Keeping this in mind, it has been categorically ruled that invasions into an individual's home requires not just reasonable suspicion, but a warrant, as all details are intimate. *Kyllo v. United States,* 533 U.S. 27, 36 (2001). However, given the fact that such a search is conducted at the border, we submit that there must exist at least reasonable suspicion, if not more.

The 'particularly offensive manner' of border searches, *Ramsey*, 431 U.S. at 618 n.13, was illustrated in *Alasaad v. Nielsen*, 2018 U.S. Dist. LEXIS 78783, where the experiences of the different plaintiffs showcased the degree of force used at the border. This 'force' and manner was used to seize the devices, or to threaten to confiscate them in order to extract their passwords. This leads to the irresistible conclusion that such an intrusive piercing invades the substantial right to privacy and dignity interests that people have – which certainly outweigh the

government's interest in conducting a forensic digital border search, devoid of reasonable suspicion. *Cotterman*, 709 F.3d at 967-968.

iii. A forensic search of an electronic device at the border would require 'reasonable suspicion' even as per precedents and directives.

The 14th Circuit's reliance on cases such as *United States v. Montoya de Hernandez*, 473 U.S. 531, (1985), *United States v. Flores-Montano*, 541 U.S. 149 (2005) and *Ramsey*, 431 U.S. 606, in order to encompass the importance of border searches never established the non-existence of the Fourth Amendment protections at the border. Rather in *Montoya,* 473 U.S. 531, a defining criterion for requiring reasonable suspicion was established in terms of non-routine border searches. In *Ramsey*, 431 U.S. 606, the courts never addressed whether the Fourth Amendment allowed suspicion-less searches. Following these cases, the precedent was set in terms of not requiring reasonable suspicion for routine border searches and thereby creating a distinct classification and requirement for non-routine searches altogether.

Having established in **I [A](i)** and **I [A](ii)** that a forensic search falls under a non-routine search at the border, the CBP Directive itself requires reasonable suspicion for the same. *See* U.S. CUSTOMS AND BORDER PROTECTION, BORDER SEARCH OF ELECTRONIC DEVICES, DIRECTIVE NO. 3340-049A (Jan. 4, 2018), https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf [*hereinafter*, 'CBP Policy 3340-049A]. Moreover, in *United States v. Vergara*, 884 F.3d 1309 (11th Circ.2018), with respect to forensic searches of electronic devices at the border, it was categorically stated that the "highest standard for a search is reasonable suspicion." *Id.* at 1313. In addition to that, Justice Jill Pryor's dissent *Vergara*, 884 F.3d (J. Pryor, J., dissenting), clearly enunciates the need

of a warrant for a forensic examination of the cell phone, keeping in mind the analysis set forth in *Riley.*

Considering the fact that the "ultimate touchstone of the Fourth Amendment is reasonableness." *Riley,* 134 S.Ct. at 2482. The argument here is similar – there must be an adherence to reasonable suspicion before a forensic examination of a cell phone can occur. Even in *Touset*, 890 F.3d at 1237, the judgement noted that there was reasonable suspicion, *a priori*. This justified the forensic search. With specific regard to Escaton, the CBP bore no reasonable suspicion whatsoever to forensically search his devices (R. at 2). Thus, it is submitted that the search conducted clearly violates the Petitioner's existing Fourth Amendment rights.

B. THE UNDERLYING JURISPRUDENCE OF THE BORDER SEARCH EXCEPTION IN TERMS OF NATIONAL SECURITY CANNOT OUTWEIGH THE REASONABLE EXPECTATION OF PRIVACY IN ELECTRONIC DEVICES.

The rationale behind the requirement of forensic searches of electronic devices at the border in terms of national security cannot be interpreted in the same manner as to that of physical objects present at the border. Data is not restricted to spatial-temporal spaces, thus it bears the capability to pose an equal threat to national security from any geographical location. The unbounded scope of acts done in pursuance of 'national security' has varied from time to time, creating an inherent contradiction of requiring probable cause in the case of FISA, 50 U.S.C.S. § 1805(a)(2)(A)(2006), whilst not requiring reasonable suspicion for a far more intrusive search at the border.

i. Threats to national security go beyond the territoriality of the border.

It has been noted that cybercrime itself is not geographically confined and "does not require physical proximity between the victim and the perpetrator." SUSAN W. BRENNER, CYBERCRIME

CRIMINAL THREATS FROM CYBERSPACE 170 (Frankie Y. Bailey, Steven Chermak, 2010). It can take place from different cities, states and countries. In light of this, the 14th Circuit's realization of national security is only considered in terms of — (i) preventing the entry of "unwanted persons and effects" (R. at 8) *Flores-Montano*, 541 U.S. at 152, and (ii) interpreting the border search exception in terms "who and what may enter the country," *Ramsey,* 431 U.S. at 620. This sets a view that the Government's interests has always been in terms of threats posed at the point of entry, thereby not paying heed to the threat faced from outside. This leads to a lack of reasonable nexus for holding that cybercrime is particularly potent only from inbound devices and data.

It is of utmost importance that the Court in this case realizes that it would be a hasty generalization to assume that devices ingress poses a greater threat to national security than those egress. The digital age has ensured that devices are equally threatening from an inbound traveler to a person located a continent away. Park, *supra* at 308. The increasing cyberattacks from China "targeting critical infrastructure (…) lay(ing) the groundwork for future disruptive attacks," Jim Finkle, Christopher Bing, *China's Hacking Against U.S. on the rise: U.S. intelligence official*, Reuters (December 11th 2018) https://www.reuters.com/article/us-usa-cyber-china/chinas-hacking-against-u-s-on-the-rise-u-s-intelligence-official-idUSKBN1OA1TB.html, is a clear example of the spatial temporal vacuum being used in favor to threaten the national security, without being physically present at the border or even around the vicinity of it. Thus 'reasonability' is a minimum threshold to prevent arbitrary and permeating searches at the border. Without such a criterion being set, there would be no protection against deep infiltrating searches of electronic devices under the claim of national security.

ii. <u>A forensic search of digital devices for the purposes of national security is not reasonably tethered to the narrow scope of the border search exception.</u>

As explained in **I [A]**, the nature of electronic devices in terms of storing data are significantly different from physical objects. In the era of *Pax Technologica* — data, digitization, and technology itself is evolving at an extremely rapid pace. Albrecht Mahr, *Transrational Peaces and Pax Technologica: On Artificial Intelligence, Peace Studies and Systemic Constellation Work*, in TRANSRATIONAL RESONANCES: ECHOES TO THE MANY PEACES 151, 154 (Springer, 2018). Cloud computing and data storage on the cloud has become of crucial relevance to the digital world. With these advances, any form of 'contraband' can thus be stored remotely in the cloud. As per the CBP Policy 3340-049A, Border Patrol agents would be required to either disable network connectivity themselves, or require the traveler to do so. As a consequence, losing access to the cloud which is beyond their purview. If the purpose of border search in terms of technological advancement is to find digital contraband for national security purposes, it would be illogical to look for it where it can be rarely found, especially at the cost of one's privacy.

Similarly, the narrow purposes of the border search exception in terms of national security is to prevent the "<u>entry</u> of unwanted persons and effects." *Flores-Montano*, 541 U.S. at 152. In terms of contraband being defined, digital contraband or data "is borderless and can be accessed and viewed in the United States without ever having crossed a physical border." *Vergara*, 884 F. 3d at 1317 (Pryor, J., dissenting). The spatial temporal irrelevance in digital data allows it to enter or leave the United States without crossing a border, or being bound by territoriality. Thus the search for digital contraband at the border is not reasonably tethered to the border such

exception itself. As such a search does not have a link "to the particular purposes served by the exception," *Florida v. Royer*, 460 U.S. 491, 500 (1983).

Although there exists a diminished expectation of privacy at the border, it cannot be said that there is no expectation of privacy at all. Even under the diminished sphere of privacy, the government cannot "justify eviscerating all protections against searches of massive scope and duration." Sid Nadkarni, "*Let's Have a Look, Shall We?" A Model for Evaluating Suspicionless Border Searches of Portable Electronic Devices*, 61 UCLA L. Rev. 146, 191 (2013). It is valuable to note that even under the government's FISA (Foreign Intelligence Surveillance Act) program, a probable cause requirement is needed before any electronic search takes place to determine whether there exists any threat posed by either foreign spies or foreign powers. Whilst both are done in order to protect the national security; one is with probable cause, and the other without even requiring reasonable suspicion. 50 U.S.C. § 1805(a)(2)(A) (2006).

C. The circumventing policy of ICE acts as a perversion to the precedents establishing reasonable expectation of privacy.

The CBP Policy 3340-049A was implemented taking into consideration the jurisprudence regarding technological advancements and privacy. Furthermore, it was intended to be executed with the objective of gaining public trust. The object of the Policy was thus to protect citizens from 'unreasonable' searches and seizures, and to ensure that the Fourth Amendment protections regarding privacy remain intact.

However, the prerogative of protecting one's privacy falls short when it remains only policy on paper, and there is a circumvention in the execution. The Policy is only applicable to the CBP agents and not the ICE agents, where both are often situated at the border simultaneously.

Keeping this in mind, when Officer Stubbs handed the phone over to the ICE Agent for a forensic search (R. at 3), the CBP Policy 3340-049A became ineffective towards Agent Cullen, where the ICE 2009 Directive applied to her. It is to be noted that the ICE 2009 Directive is still effective and has not been updated on par with the CBP Policy. This grants unfettered powers to ICE agents to forensically search electronic devices, without having reasonable suspicion, and also permits them to access cloud networking data. In its breadth and reach, it is significantly wider and far more permeating.

Even a forensic examination of electronic devices entails copying the contents of the device for "further review either on-site at the place of detention or at an off-site location," *See* ICE 2009 Directive, which can take place beyond the physical search at the border itself. *United States v. Saboonchi*, 990 F. Supp. 2d 536. The Court in *U.S.A vs. Kim*, No. 13-cr-00100-ABJ, 2015 BL 134375 (D.D.C. May 8, 2015), addressed this matter, where a forensic search of electronic devices was conducted at an off-site location without reasonable suspicion. In this regard, the Court held that the evidence was liable to be suppressed. However, the ICE 2009 Directive is in contrast to the CBP Policy 3340-049 in terms of a forensic search being taken place without having established the reasonable suspicion standard, thereby allowing the ICE agents to send the device to an off-site facility for a period of 30 days. *See* ICE 2009 Directive.

In the case at hand, there has been an express handover of Escaton's devices to Agent Cullen (R. at 3) who is not bound by the protocol and protections of the CBP Policy 3340-049. Thus, in effect, circumventing the drafter's intent to maintain privacy protections even during digital searches. It is thus submitted that this Court realize this inconsistency in the policies which allows a perverse interpretation and permits unreasonable searches impinging on one's privacy.

II. THE USE OF CELL SITE LOCATION INFORMATION OBTAINED BY LAW ENFORCEMENT CONSTITUTED AN 'UNREASONABLE SEARCH' AND IMPINGED ON THE 4TH AMENDMENT RIGHTS OF THE PETITIONER.

A. THE PETITIONER BORE A CONSTITUTIONALLY RECOGNIZED EXPECTATION OF PRIVACY IN HIS MOVEMENTS THAT WAS SUBJECTIVELY AND OBJECTIVELY REASONABLE.

As per the Fourth Amendment of the United States Constitution, Escaton has a right to be secure against "unreasonable" searches as to his "persons, houses, papers, and effects." U.S. CONST. amend. IV. Further, an intrusion on any person's reasonable expectation of privacy would trigger a violation of their rights under the provision. *Katz v. United States*, 389 U.S. 347, 351 (1967). While the essence of this provision does not seemingly take into account technological advancements, the jurisprudence of the Supreme Court has allowed this provision to apply with changing times. Where in the case of *Riley*, 134 S. Ct. at 2490, it was seen that cell phones are "qualitatively different" with regard to the wealth of information they provide.

i. ***Carpenter*** **has expressly recognized that acquiring historical CSLI without a warrant violates a person's reasonable expectation of privacy**

The Court in *Carpenter v. USA,* 138 S. Ct. 2206 (2018)*,* was confronted with the question of "long-term surreptitious tracking (*Jones*) by a uniquely powerful device (*Riley*) capable of near-perfect surveillance." Susan Freiwald & Stephen Wm. Smith, *The Carpenter Chronicle: A Near Perfect Surveillance*, 132 HARV. L. REV. 205, 216 (2018) (discussing the decision and impact of the case). It answered by categorically stating that individuals have a "reasonable expectation of privacy in the whole of [their] physical movements," *Carpenter*, 138 S. Ct. at 2219, and that a warrant is required in such cases where a legitimate privacy interest exists. Further, stating that such data is beyond the scope of the third party doctrine, the Court also acknowledged that CSLI is a "different species of business record(s)." *Id*. at 2222.

Several other factors were considered with regard to technological advancement and CSLI that implicated the Fourth Amendment — intrusiveness, continuity, hiddenness, indiscriminate nature of collection, expense and efficiency. *Id*. CSLI is not by nature, a tool created for law enforcement, it has been made one. In *Kyllo,* 533 U.S. 27, it was noted that thermal imaging instruments were not in "general public use." *Id*. at 34. This played an important factor in leading to the decision that a warrant was needed, as such tools intruding on privacy were not otherwise accessible.

With regard to Escaton's case, though *Carpenter,* 138 S. Ct. 2217, n.3, did not expressly address the issue of obtaining historical CSLI for fewer than seven days, it is to be noted that the majority did not seek to address the 'limited period' that may be needed for Fourth Amendment scrutiny to apply. *Carpenter,* 138 S. Ct. 2217, n.3; Transcript of Oral Argument at 7, 11, Carpenter v. USA, 138 S. Ct. 2206 (No. 16-402). Several cases hence have followed the ruling, extracting the critical rationale, that warrantless tracking of an individual's location is opposed to the Fourth Amendment, irrespective of the "amount of time the government seeks to monitor that particular person." *People v. Simpson*, 2018 NY Slip Op 28371 (Sup. Ct.) (holding that the distinction between obtaining seven days of CSLI from three days was *de minimis*); *United States v. Beverly,* No. Criminal H-16-215-1, 2018 U.S. Dist. LEXIS 183539 (S.D. Tex. Oct. 25, 2018); 2018 WL 5297817; *State v. Brown*, No. A-17-365, 2018 Neb. App. LEXIS 40 (Ct. App. Mar. 6, 2018). Further, it has been historically noted that the Supreme Court has found any warrantless search within the home, "presumptively unreasonable." *United States v. Karo*, 468 U.S. 705, 715 (1984) (quoting *Welsh v. Wisconsin*, 466 U.S. 740 (1984)).

Thus, notwithstanding the fact that the Court sought to obtain three days of historical CSLI as opposed to the seven days in *Carpenter*, 138 S. Ct. 2206, it is humbly submitted that the scope and rationale of the judgement recognizes the right to privacy as it exists with regard to an individual's locational information. This, along with the other rubrics aforementioned, leads to the irresistible conclusion that the data obtained via the three-day CSLI requests are to be suppressed. Else, there would be an obliteration of Escaton's right to privacy, recognized under the Fourth Amendment. Further, the two primary considerations remain the fact that there is a need to prevent: (i) arbitrary encroachments on the right to privacy; and (ii) permeating police surveillances. *Carpenter*, 138 S. Ct. 2214. With increasing precision and accuracy in data obtained from cell towers [**I A(ii)**], the aforementioned considerations are at their zenith.

Though the 14th Circuit though it proper to defer the matter to Congress for determining the standard under the ECPA Modernization Act of 2017, it is necessary that there is no circumvention of justice in the bargain. A similar view prompting the legislature to enact necessary protections was considered in *Riley,* 134 S. Ct., and in *Jones,* 565 U.S. 400. Despite this, it has been the case that this Supreme Court has recognized the importance of cell phones, privacy, and technological advancement almost concurrently with Congress. This includes addressing issues of wiretapping, *Katz*, 389 U.S. 347, thermal imaging, *Kyllo*, 533 U.S. 27, censorship of pornographic television shows, *United States v. Playboy Entm't Grp.*, 529 U.S. 803 (2000), and now issues concerning "minicomputers" that seem to be compulsively carried everywhere. *Riley*, 134 S. Ct. at 2489.

ii. <u>Escaton sought to preserve his location as private, though he was in an area accessible to the public.</u>

It has been long recognized since *Katz,* 389 U.S. 347, that the mere fact that an individual is in a public space does not take away his Fourth Amendment rights. Holding, "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id*. at 351. Similarly, the Weekday Records seeking 10-days of CSLI during 8:00 AM to 6:00 PM (MDT) violated Escaton's reasonable expectation of privacy. This is notwithstanding the argument that Escaton could have been operating during working-hours on public thoroughfares. Showcasing the first pillar of Fourth Amendment jurisprudence — reasonable expectation of privacy.

The rationale of *Carpenter,* 138 S. Ct. at 2266*,* was to place limits on 'arbitrary power' and 'place obstacles' on permeating police surveillances. To interpret the case to reflect that one bears a reasonable expectation of privacy only when there is an intrusion beyond '168 hours' would lead to a perverse interpretation of the case. Further nowhere is there any mention that seven days of surveillance necessarily means 168 hours of CSLI. Neither was there a mention that such time period is to be calculated in seriatim. The consideration was simple, it was a matter of sketching a "near perfect surveillance." *Id*. at 2210. The same rubrics articulated in [**II A(i)**] also apply to the 10-day records of CSLI, impinging on Escaton's Fourth Amendment rights. It is a maxim often noted that 'what cannot be done directly, cannot be done indirectly'. *Cummings v. Missouri* (1867) 71 U.S. 277, 325 (stating further that the Constitution deals with substance, not shadows); s*ee generally,* D.K. Singh, *"What Cannot be Done Directly Cannot be Done Indirectly": Its Meaning and Logical Status in Constitutionalism*, 29 Mod. L. Rev. 273 (1966).

As noted by *Justice Weber* in the 14th Circuit, historical CSLI allows law enforcement "to travel back in time to retrace a person's whereabouts," (R. at 16) effectively allowing it to be a tool with retrospective effects. In addition to this consideration, with developing technology, there exist algorithms that refine and predict future movements and patterns of behavior with historical CSLI data, thus serving as a prospective surveillance and profiling tool as well. David Talbot, *A Phone that Knows Where You're Going*, MIT TECHNOLOGY REVIEW, Jul. 9, 2012, <https://www.technologyreview.com/s/428441/a-phone-that-knows-where-youre-going/>.

Further, there exists literature to prove that due to urban density and changing times, CSLI now includes "microcell-, picocell-, and femtocell- generated data," Stephanie K. Pell, *Location Tracking*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 44–70 (David Gray & Stephen E. Henderson eds., 2017), which only increases the precision of historical CSLI over time. In this case, it is clear that Sweetwater is densely populated with numerous cell towers (R. at 22), which heightens the accuracy of the historical cell site data obtained, rather than to say the information is imprecise (R. at 13). Thus law enforcement's tracking of Escaton is clearly permeating, arbitrary, and excessive.

It was held in the 14th Circuit that the Weekday Records spanning over ten days for 100 hours does not capture a 'near perfect surveillance' (R. at 13). However this is unsustainable as individuals do expect some a degree of anonymity in public, which may not involve 'illegal' activities, but certainly impinge on their liberties. A similar argument that once an individual is in public, operating on public thoroughfares, they lose their reasonable expectation of privacy was categorically rejected in *United States v. Jones,* 565 U.S. 400 (2012). Here, it was recognized that there existed "constitutionally protected area[s]," *Id*. at 407, n.3, and an intrusion thereof would

inevitably lead to a 'search'. U.S. CONST. amend. IV. Thus, emphasizing the other pillar of Fourth Amendment jurisprudence — trespass. This further ties into the argument related to property rights-based theory, and common law trespass **[iii]**.

iii. <u>The property rights-based theory of the Fourth Amendment dictates that Carpenter had a reasonable expectation of privacy as to the data in his cell phone.</u>

Justice Gorsuch's dissent in *Carpenter* provides a valuable insight into the "traditional property-based understanding of the Fourth Amendment." *Carpenter*, 138 S. Ct. at 2268 (Gorsuch, J., dissenting). The "unpredictable (…) and unbelievable jurisprudence," *Id*. at 2266 (Gorsuch, J., dissenting), as a consequence of *Katz* mandated considering the proprietary framework once again. In *United States v. Ackerman,* 831 F.3d 1292 (10th Cir. 2016), the Court synthesized the principles in *Katz,* 389 U.S. at 360 (reasonable expectation of privacy), and in *Jones,* 565 U.S. at 400 (common law trespass test*),* to conclude that Fourth Amendment protections would be available when either of these doctrines were violated — thus reintroducing the familiar jurisprudence of common law trespass to the Fourth Amendment. The case clearly held that the Defendant had a property interest in his emails, and had a reasonable expectation of privacy in the same.

Similarly, with regard to the Petitioner's case, the provisions of the Wireless Communications and Public Safety Act, 47 U.S.C. §§ 609-615b (1999), enacted by Congress provides for insight into the congressional intention that proprietary information includes an individual's location. As per the Act, 'proprietary network information', includes the location information of a customer. 47 USC § 222(h)(1) (1999). This, along with the right of the customer to recover damages indicates that the CSLI comes within the realm of a proprietary interest. 47 U.S. Code § 207 (1999). It has been argued that the positive law model can be realized by taking this proprietary

framework even further. The exception engrafted to maintaining privacy provides for disclosure, if mandated by the Government. This "government exceptionalism" triggers the positive law model to realize that searches by the government have an equal bearing on personal security. William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821 (2016). However, it is submitted that rather than enforcing the positive law model regarding government trespass *in toto*, the proprietary framework even in a minimal sense, mandates the procurement of a warrant before such encroachments are made.

In effect, Escaton bears a property interest in the digital data associated to his cellphone, where the CSLI information is obtained through the "modern-day equivalents," *Carpenter*, 138 S. Ct. at 2222, of 'papers' or 'effects'. Additionally, *United States v. Knotts,* 460 U.S. 276 (1983) and *United States v. Karo,* 468 U.S. 705 (1984), had earlier laid down a foundation for digital trespass, further elucidated by *Jones*, 565 U.S. 400, thematically indicating that law enforcement "cannot turn a person's property into an informant." Hannah Lichtig Cook, *(Digital) Trespass: What's Old is New Again*, 94 DENV. L. REV. ONLINE 165, 171 (2017). Further, as noted by Justice Gorsuch, there is a significant expansion of the traditional notions of 'property' to include digital data and assets. *Carpenter*, 138 S. Ct. at 2270 (Gorsuch, J., dissenting). The common law principle of trespass would certainly support the notion that even a day's worth of CSLI obtained without a warrant would amount to a trespass on this 'digital data' emitted in the form of signals.

B. THE ROBUSTNESS OF THE THIRD PARTY DOCTRINE HAS SHIFTED POST-*CARPENTER*, THUS MANDATING A WARRANT BEFORE CSLI CAN BE ACCESSED FROM TOWER DUMPS.

After *Carpenter v. USA*, 138 S. Ct. at 2222, it became clear that there was a significant shift in the operation of the third-party doctrine as put forth in *Smith v. Maryland, 442 U.S. 735 (1979),*

and *United States v. Miller*, 425 U.S. 435 (1976), where the Supreme Court declined to extend its application to CSLI. Most of the decisions prior to this shift in the robustness of the doctrine had allowed for acquiring CSLI through the SCA, which does not require a warrant. The shift needs to be acknowledged as several cases relied on this third party doctrine to declare that a warrant was unnecessary for obtaining data from tower dumps. *In re* United States, 42 F. Supp. 3d 511, 512-14, 519-20 (S.D.N.Y. 2014); *In re Cell Tower Records Under 18 U.S.C. 2703(d)*, 90 F. Supp. 3d 673 (S.D. Tex 2015). Even the 14th Circuit's reliance on *United States v. Pembrook*, 119 F. Supp. 3d 577 (6th Cir. 2017), (R. at 14) needs to be reconsidered. The case contemplated there being no 'binding authority' that necessitated a warrant requirement to access cell-site data revealing locational information of an individual. *Id*. at 587. However, it is clear that an individual now bears a reasonable expectation of privacy in the 'whole' of their physical moments. *Carpenter*, 138 S. Ct. at 2219.

Records concerning locational information cannot be characterized as business records *simpliciter*. With this distinct nature of CSLI, the information obtained from the tower dumps are liable to be suppressed because they fall within the realm of 'arbitrary' searches **(i)**. Further, the protocol for seeking tower dump data confers minimal Fourth Amendment protection, which allows for a fishing expedition **(ii)**.

i. <u>Tower dumps are subset of historical CSLI whose usage sanctions arbitrary power</u>

Tower dump data is obtained by law enforcement primarily at the initial stages of an investigation to obtain data relating to devices connected to a particular cell tower. One of the main legitimate apprehensions associated to such data is its capability of acting as a "digital dragnet." JAMES P. MARTIN & HARRY CENDROWSKI, CLOUD COMPUTING AND ELECTRONIC

DISCOVERY 97 (John Wiley & Sons, 2014). There is a wealth of information obtained, sometimes adding up to even '150,000 registered cell phone(s)'. *Id*. at 94. Though it is unable to sketch an 'intimate window' (R. at 12) of a particular individual's life — it certainly still falls within the realm of a tool bearing "arbitrary power." *Carpenter*, 138 S. Ct. at 2214 (quoting *Boyd v. United States*, 116 U.S. 616 (1886)). This is in light of the fact that such data is obtained through increasingly simple ways due to technological advancement and new surveillance tactics. *Jones,* 565 U.S. at 414. With such drastic developments and weak standards to prevent arbitrary encroachment, there is a clear erosion of privacy rights.

It has also been noted by District Judge, Nicholas Garaufis, that cell location data obtained from tower dumps permits 'mass' electronic surveillance that significantly amplifies Fourth Amendment concerns. *In re United States for an Order Authorizing the Release of Historical Cell-Site Info*., 809 F. Supp. 2d 113, 119 (E.D.N.Y. 2011). For the purposes of such wholesale surveillance, it was held that individuals have a legitimate reasonable expectation of privacy due to the constitutional concerns associated to such a magnitude of intrusiveness. With the data obtained from three tower dumps (R. at 4), law enforcement could triangulate and obtain the geographical location of several users. Pell, *supra* at 49.

Further, as analyzed in **II A(iii)**, one bears a certain legitimate property-interest in the data concerning their location information. This applies even to tower dumps, more so considering that the data obtained affects a large number of people. For instance, if there is a situation where the tower dump data has been obtained for an individual in an area serving an Alcoholics Anonymous meeting, or visiting a site of religious location — this would have extremely

problematic outcomes. *See* RONALD J. ALLEN, ET AL., COMPREHENSIVE CRIMINAL PROCEDURE 397 (Wolters Kluwer Law & Business, 3rd ed. 2011).

ii. <u>A warrant does not pose an additional burden on law enforcement, it merely prevents a fishing expedition.</u>

The Court in *Riley,* 134 S. Ct. at 2495, realized that technological changes mandate a review of the protections under the Fourth Amendment, which are relevant and necessary. Though tower dump data might be useful in the initial stages of investigation, it would be a fishing expedition to allow law enforcement to obtain such data without a higher degree of scrutiny. Especially considering how in the current day and age, individuals "compulsively carry cell phones with them all the time." *Carpenter*, 138 S. Ct. at 2218. The argument that this tool of surveillance can be likened to security cameras or E-Z pass monitors (R. at 14) is incorrect, as it has scope for varied usage than the narrow purposes of the aforementioned two devices. The data is generated based on the automatic connection of a cellphone to a particular tower in the vicinity. It is converted into a tracking device for the purposes of law enforcement, where the data is obtained from a third party.

The prospective and retrospective nature of historical CSLI, has been earlier argued **[II A(ii)]**, where the triangulation methods of location accuracy raise similar concerns. With regard to tower dumps, there are further considerations regarding the nature of sensitive data revealed for individuals *en masse*. The Supreme Court of Canada was confronted with the same question in *R v. Mahmood*, [2011] ONCA 693 (Can.). It was observed that data obtained through tower dumps, without a warrant, was said to contravene S. 8 of the Canadian Charter, protecting personal privacy. In this case, it was seen that the tower dump requests constituted a "high-tech 'fishing

expedition' (…) in the hope that some information would be obtained that would permit the police investigation to move forward." *Id*. at ¶ 72.

Similarly, this Court's stance with regard to fishing expeditions was well elucidated in *FTC v. Am. Tobacco Co.,* 264 U.S. 298 (1924)*,* here it was held that a fishing expedition into the papers of a corporation on the mere "possibility that they may disclose evidence of crime, is so contrary to first principles of justice." *Id*. at 306. Thus, to balance the needs of law enforcement and the privacy interest of individuals, when the government seeks to acquire "modern-day equivalents of (…) papers and effects," *Carpenter*, 138 S. Ct. at 2222, it is clear that they should proceed only with a warrant. Thus with less human labour and associated costs, technology as it exists today, comes with inbuilt tracking devices that has drastically increased the government's surveillance powers. Pell, *supra* at 58.

C. THE 'GOOD FAITH' EXCEPTION TO THE EXCLUSIONARY RULE DOES NOT APPLY, AND THE EVIDENCE SHOULD BE SUPPRESSED .

Carpenter, 138 S. Ct. at 2219, laid down the precedent that an individual has a reasonable expectation of privacy in their physical movements. While recognizing the requirements under the SCA, the Court believed that those standards were a "gigantic departure," *Id*. at 2221, from the probable cause standard. Thus, to the extent that the government could have obtained CSLI without a warrant under the SCA, the Supreme Court held the provisions to be unconstitutional. *See United States v. Curtis*, 901 F.3d 846, 848-850 (7th Cir. 2018).

The 'good faith' exception to the exclusion of warrantless CSLI was applied in cases after acknowledging that the information procured was in contravention to the Fourth Amendment, where the motion to suppress was disregarded, keeping this exception in mind. However, the

cases applying this exception was chronologically prior to the categorical pronouncement of the rule in *Carpenter* in 2018, where law enforcement did not have to adhere to a binding precedent. This was noted in *United States v. Chambers*, No. 16-163-cr, 2018 U.S. App. LEXIS 27073 (2d Cir. Sep. 21, 2018) (holding that "the extent the government relied on an SCA order to procure the data at did not comport with the Fourth Amendment"). However, based on the facts and circumstances of the case at hand, the location information for Escaton concerning the — **(i)** Tower Dump Data, **(ii)** Three days of CSLI, and **(iii)** Weekday Records, were all obtained post September 25th, 2019 (R. at 2). Thus, well beyond the ruling of *Carpenter*, and it's jurisprudence mandating a warrant.

As a consequence, law enforcement had knowledge that they would be contravening the Petitioner's realized and legitimate expectation of privacy. Further, the mandate that such data requires a warrant based on probable cause was clear. Thus, the Petitioner's motion to suppress such data should be upheld in this Honorable Court, as the evidence was not obtained in good-faith reliance on the SCA to the extent of its unconstitutionality as declared by *Carpenter*.

CONCLUSION

There was a violation on the Petitioner's Fourth Amendment rights. Based on the arguments hereinbefore presented, first, there existed no reasonable suspicion to conduct a forensic search of the Petitioner's electronic devices at the border. This search was intrusive, particularly offensive, and non-routine. Second, the data obtained via cell site location information and tower dumps required a warrant as it was a Fourth Amendment search. The Petitioner bore a subjective and objective expectation of privacy against arbitrary and unreasonable searches. For these reasons, the Petitioner requests this Court to REVERSE the decision of the Fourteenth Circuit, and allow for the motion to suppress evidence.

Respectfully submitted,

Attorneys for Petitioner.