No. 15-3996

IN THE

Supreme Court

of the United States

GERRARD LEOMUND,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Writ of Certiorari to
the United States Court of Appeals
for the Fourteenth Circuit

BRIEF FOR RESPONDENT

Team 14
Counsel for the Respondent

January 11, 2016

45th Annual William B. Spong, Jr. Moot Court Tournament

QUESTIONS PRESENTED

I. Whether the Computer Fraud and Abuse, through the phrase "without authorization," imposes a use restriction, in light of the statute's plain language and legislative history strongly suggesting the statute forbids the unauthorized use of a computer.

II. Whether the Computer Fraud and Abuse Act, through the phrase "exceeds authorized access," should ground liability in agency principles and contract law, two sources that have traditionally defined the employer-employee relationship.

III. Whether the Court should adopt the mosaic approach to the Fourth Amendment, which considers whether government action in the aggregate violates an individual's reasonable expectation of privacy, despite the Court's successful history of protecting Fourth Amendment rights using a discrete, sequential approach.

TABLE OF CONTENTS

QUESTIONS PRESENTED i

TABLE OF AUTHORITIES v

OPINIONS BELOW 1

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED..... 1

STATEMENT OF THE CASE 2

Statement of the Facts 2

Procedural History 4

SUMMARY OF THE ARGUMENT 4

ARGUMENT 7

I. THE PLAIN WORDING AND LEGISLATIVE HISTORY OF THE COMPUTER FRAUD AND ABUSE ACT SUGGEST THAT CONGRESS, THROUGH THE PHRASE "WITHOUT AUTHORIZATION," INTENDED TO PROHIBIT THE UNAUTHORIZED USE OF A COMPUTER 7

A. The CFAA's Plain Language Prohibits the Unauthorized Use of a Computer 8

B. The CFAA's Legislative History Prohibits the Unauthorized Use of a Computer 10

C. Under the Facts of This Case, Petitioner Acted Without Authorization When He Misused the Computer 12

II. THE AGENCY AND CONTRACT-BASED APPROACHES TO THE COMPUTER FRAUD AND ABUSE ACT SUPPORT THE NOTION THAT CONGRESS, THROUGH THE PHRASE "EXCEEDS AUTHORIZED ACCESS," INTENDED TO PROHIBIT THE UNAUTHORIZED USE OF A COMPUTER 13

A. The Agency-Based Approach Provides a Persuasive Reason to Adopt the Broad Interpretation of the Phrase "Exceeds Authorized Access" 14

1. THE AGENCY-BASED APPROACH 14

2. THE REASONS WHY THE COURT SHOULD ADOPT THE AGENCY-BASED APPROACH 15

3. UNDER THE FACTS OF THIS CASE, PETITIONER EXCEEDED HIS AUTHORIZED ACCESS WHEN HE VIOLATED HIS AGENCY RELATIONSHIP……. 15

B. The Contract-Based Approach Provides an Additional Persuasive Reason to Adopt the Broad Interpretation of the Phrase "Exceeds Authorized Access"……..……. 16

1. THE CONTRACT-BASED APPROACH …….. 16

2. THE REASONS WHY THE COURT SHOULD ADOPT THE AGENCY-BASED APPROACH..… 17

3. UNDER THE FACTS OF THIS CASE, PETITIONER EXCEEDED AUTHORIZED ACCESS WHEN HE VIOLATED HIS CONTRACT …….. 17

III. PETITIONER'S MOTION TO SUPPRESS WAS CORRECTLY DENIED BECAUSE THE GOVERNMENT'S ACTIONS WERE INDIVIDUALLY CONSTITUTIONAL, THE MOSAIC APPROACH IS AN IMPERMISSIBLE ANALYSIS OF FOURTH AMENDMENT PROTECTIONS, AND, EVEN IF IT IS APPLIED IN THIS CASE, THE GOVERNMENT'S ACTIONS DO NOT VIOLATE A REASONABLE EXPECTATION OF PRIVACY.……..... 18

A. This Court Should Not Adopt the Mosaic Approach…….....…..……... 20

1. THE SUPREME COURT HAS SUCCESSFULLY UTILIZED THE SEQUENTIAL APPROACH TO DEFEND FOURTH AMENDMENT RIGHTS TIME AND AGAIN, AND THERE IS NO CONTEMPORARY NEED TO CHANGE ITS VERY NATURE……...…..... 20

i. Maynard, Jones, and the Mosaic Approach ……...……..……. 20

ii. The Sequential Approach ……...……..……. 21

iii. The Sequential Approach Effectively Protects Fourth Amendment Rights ……... 23

2. THE MOSAIC APPROACH WILL INVALIDATE FIRMLY ESTABLISHED, CONSTITUTIONAL INVESTIGATORY TECHNIQUES …….. 24

3. THE MOSAIC APPROACH WILL PRESENT AN UNWORKABLE STANDARD FOR COURTS, REQUIRING THEM TO ANSWER NUMEROUS QUESTIONS THAT HAVE ALREADY BEEN SETTLED UNDER THE SEQUENTIAL APPROACH, AND REQUIRING THEM TO ANSWER DIFFICULT LINE-DRAWING QUESTIONS FOR WHAT CONDUCT IS PERMISSIBLE UNDER THE FOURTH AMENDMENT …….……. 26

4. THE MOSAIC APPROACH IS AN UNWORKABLE STANDARD THAT DISABLES COURTS FROM PROVIDING EFFECTIVE REMEDIES FOR FOURTH AMENDMENT VIOLATIONS …… 29

B. Even if This Court Does Adopt the Mosaic Approach, the Government's Actions in This Case Are Not Rendered Unreasonable Under the Fourth Amendment When Considered Cumulatively or in the Aggregate 31

1. THE MOSAIC APPROACH IS GROUNDED IN THE NOTION THAT PROLONGED INVESTIGATIONS PAINT AN INTIMATE PICTURE OF AN INDIVIDUAL'S LIFE 32

2. HERE, THE GOVERNMENT'S ACTIONS DO NOT PAINT A COMPREHENSIVE OR INTIMATE PICTURE OF PETITIONER'S LIFE SUFFICIENT TO CONSTITUTE A SEARCH 34

i. The Government Did Not Acquire Sufficiently Intimate or Comprehensive Information 34

ii. The Duration of the Government's Investigation was Insufficient to Implicate Mosaic Theory Fourth Amendment Concerns 35

3. EVEN IF THE MOSAIC APPROACH HERE DOES PROVIDE AN INTIMATE PICTURE OF PETITIONER'S LIFE, SOCIETY HAS NO REASONABLE EXPECTATION OF PRIVACY IN LOCATION DATA IN TODAY'S INCREASINGLY ADVANCED TECHNOLOGICAL WORLD 37

CONCLUSION 40

TABLE OF AUTHORITIES

Cases

Arizona v. Evans, 514 U.S. 1 (1995) 33

California v. Ciraolo, 476 U.S. 207 (1986) 26

CollegeSource, Inc. v. AcademyOne, Inc., 597 F. App'x 116 (3d Cir. 2015) 7

Consumer Product Safety Commission et al. v. GTE Sylvania, Inc. et al., 447 U.S. 102 (1980) ... 8

Davis v. United States, 131 S. Ct. 2419 (2011) 33, 34

EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001) 7, 19

Herring v. United States, 555 U.S. 135 (2009) 33, 34

Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006) 7, 9, 16

Katz v. United States, 389 U.S. 347 (1967) 21, 22, 25, 28

Kyllo v. United States, 533 U.S. 27 (2001) 27

Miller v. United States, 357 U.S. 301 (1957) 25

New York v. Class, 475 U.S. 106 (1986) 26

Olmstead v. United States, 277 U.S. 438 (1928) 25

Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295 (6th Cir. 2011) 8

Ransom v. FIA Card Servs., N.A., 131 S. Ct. 716 (2011) 10

Smith v. Maryland, 442 U.S. 735 (1979) 22, 26

Terry v. Ohio, 392 U.S. 1 (1968) 25

United States v. Cuevas-Perez, 640 F.3d 272 (7th Cir. 2011) 36

United States v. Graham, 846 F. Supp. 2d 384 (D. Md. 2012) 42

United States v. Jacobsen, 466 U.S. 109 (1984) 31

United States v. John, 597 F.3d 263 (5th Cir. 2010) 7

United States v. Jones, 132 S. Ct. 945 (2012) ..... passim

United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) 23, 28, 29, 37

United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) 8

United States v. Phillips, 477 F.3d 215 (5th Cir. 2007) 14, 15

United States v. Teague, 646 F.3d 1119 (8th Cir. 2011) 7

WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012) 7, 8

Statutes

18 U.S.C. § 1030(a)(2)(B) (2008) 8

18 U.S.C. § 1030(a)(7) (1996) 11

18 U.S.C. § 1030(e)(6) (2006) 9, 15

Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, 98 Stat. 1837 (1984) 10

Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (1986) 10

Former Vice President Protection Act, Pub. L. No. 110-326, 122 Stat. 3560 (2008) 12

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) 12

Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-122, 108 Stat. 1796 (1994) 11

Other Authorities

Entitle Definition, *Black's Law Dictionary* (9th ed. 2010) 16

Garrett Urban, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52 Wm. & Mary L. Rev. 1369, 1388 (2011) 17

H.R. Rep. No. 99-612 (1986) 11

Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311, 315 (2012). ..... passim

Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1561 (2010) 13

Orrin S. Kerr, *Fourth Amendment Remedies and Development of the Law: a Comment on Camreta v. Greene and Davis v. United States*, 2011 Cato Sup. Ct. Rev. 237, 241-42 (2011). 34

Orin S. Kerr, *Obama's Proposed Changes to the Computer Hacking Statute: A Deep Dive*, Volokh Conspiracy (Jan. 14, 2015), http://www.washingtonpost.com 14

S. Rep. No. 99-432 (1986) 11, 12

U.S. Dep't of Justice, *Prosecuting Computer Crimes* 2 (2d ed. 2010), www.justice.gov 12

William J. Stuntz, *Warrants and Fourth Amendment Remedies*, 77 Va. L. Rev. 881, 900-09 (1991) 34

Treatises

73 Am. Jur. 2d Statutes § 83 (2014) 12

Restatement (Second) of Agency § 1 (1958) 14

Restatement (Third) of Agency § 1.01 (2006) 14

Constitutional Provisions

U.S. Const. amend. IV 17

OPINIONS BELOW

The United States District Court for the District of Greyhawk granted petitioner's motion to dismiss and motion to suppress in an unpublished opinion. J.A. at 13–27. The United States Court of Appeals for the Fourteenth Circuit reversed both orders. J.A. at 4–12.

CONSTITUTIONAL PROVISIONS AND STATUTES INVOLVED

U.S. Const. amend. IV

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.

The Computer Fraud and Abuse Act, **18 U.S.C § 1030 (a)(2)(B) (2008)**

(a) Whoever—

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(B) information from any department of agency of the United States…

STATEMENT OF THE CASE

Statement of the Facts

Gerrard Leomund ("Petitioner") was a statistician for the Center for Disease Control ("CDC"), where he was charged with predicting the spread of infectious diseases. J.A. at 13. After twenty years of employment, Petitioner was promoted to be an Assistant Content Director/Disease Projection Analyst. *Id.* In his new role, Petitioner was granted access to all material in the CDC-Secure Database System ("CDC-Secure Database"). J.A. at 14. Every time an employee tries to access the CDC-Secure Database, he or she must read and affirm database restrictions. *Id.* It is only after explicitly agreeing to the restrictions that the employee can log on. *Id.* One restriction prohibits employees from "[u]sing the database in a manner that violates the terms of the individual's employment with the Centers for Disease Control." *Id.*

In January 2013, the CDC began to analyze the spread of the Phyresis pathogen. *Id.* Despite the CDC's limited data on the pathogen, Petitioner demanded in a memorandum dated April 5, 2013 that the CDC release its data to the public. *Id.* Petitioner's supervisor, Dana Gant ("Gant"), refused his demand and warned that he should simply continue analyzing the pathogen. *Id.* After Petitioner again asked Gant on May 10, 2013 to release the information, she transferred him to a different department. *Id*. Following the transfer, Petitioner continued to have access to the CDC-Secure Database in order to solely study his new assignment: Alzheimer's. *Id.*

On May 14, 2013, a news report about "the Phyresis Crisis" that cited extensively to a website, www.PhyresisGate.com, came to the attention of Gant. *Id.* The report contained information about the pathogen that could only have come from the CDC-Secure Database. *Id.* Later, on May 17, 2013, Gant again saw a program regarding the Phyresis pathogen. *Id.* The CDC's technology department determined that Petitioner's credentials had been used to access

the information following his transfer. *Id.* Recognizing Petitioner's likely role, Gant began the formal process of terminating Petitioner's employment to ensure Petitioner would no longer leak information. *Id.*

In late May, after yet another release of information, Gant contacted the Federal Bureau of Investigation ("Government") to bring criminal claims against Petitioner. J.A. at 15. Noting that Petitioner finally lost access to the CDC-Secure Database because he was fired, the Government quickly reasoned that he must have been working with a co-conspirator. *Id.* On May 27, 2013, the Government set up a video camera on a telephone pole in front of Petitioner's home for a total of five days. *Id.* The camera was more than seventy-five feet away, and could not move, zoom or focus. *Id.* It also could not reveal any of the contents or activities within the home. *Id.* From the feed, the FBI saw that Petitioner left the home for most of the day, and received packages and foods. *Id.* Finding the information not helpful, the FBI removed the camera and sought another way to find the co-conspirator: license plate scanners. *Id.*

On June 1, 2013, the Government coordinated with local police to utilize license plate scanners for ten days. *Id.* The scanning occurs by pure happenstance—only cars near police cars get scanned. Here, the police recorded twelve individual "hits" of the location of Petitioner's car. *Id.* Three hits recorded the location of Petitioner's car on state roadways, three at gentlemen's clubs, two at a grocery store, two at a psychiatrist's office, one at a urologist's office, and one at a nearby restaurant. *Id.* The police took one of the roadway scans at a location behind Petitioner's home. J.A. at 16. On June 12, 2013, an officer on that road observed the arrival of a new car. *Id.* The police had finally found their co-conspirator.

On June 12, 2013, the Government, in order to observe Petitioner meeting the co-conspirator, dispatched a drone equipped with a digital camera. *Id.* Given the great size of

Petitioner's home, the drone had to fly for twenty minutes at an altitude of 400 feet to find the individuals. *Id.* Zooming in, the Government saw Petitioner meeting with one of the CDC's Disease Topography Specialists. *Id.* They were sitting outside in the back yard. Sprawled over their table was a CDC specialty contoured disease map. *Id.* The Government quickly obtained an arrest warrant and arrested the two men. Petitioner confessed to accessing the CDC-Secure Database to update his website. *Id.*

Procedural History

The Government charged Petitioner with violating the Computer Fraud and Abuse Act ("CFAA"). In response, Petitioner filed a motion to dismiss and to suppress all evidence obtained in the Government's investigation. The United States District Court for the District of Greyhawk ("District Court") granted both motions. J.A. at 13–27. The United States Court of Appeals for the Fourteenth Circuit ("Court of Appeals") reversed both decisions. J.A. at 5–12. The Supreme Court granted certiorari regarding whether Petitioner violated the CFAA, and whether the Government's investigation comports with the Fourth Amendment.

SUMMARY OF THE ARGUMENT

The Court of Appeals' decision to deny Petitioner's motion to dismiss should be affirmed because the court correctly adopted a broad reading of the CFAA, and rejected the mosaic reading to the Fourth Amendment. A broad reading of the CFAA makes sense in light of its plain language and legislative history—but a broad reading of the Fourth Amendment through the mosaic approach violates Supreme Court precedent and protects too many potential criminals from reasonable searches.

This Court should adopt a broad reading of the CFAA. First, the plain language is clear: the phrases "without authorization" and "exceeds authorized access" are synonymous. When an

individual exceeds authorized access, he or she is by definition without authorization. The CFAA defines the phrase "exceeds authorized access" in a way that prohibits unauthorized use. The statute imposes liability on an individual who "obtains or alters" information he or she was not "entitled so" to obtain or alter—suggesting a use restriction. Furthermore, the legislative history evinces Congress's strong desire to impose a use restriction. For one, the original CFAA explicitly imposed a use restriction. Though the language establishing a use restriction was deleted, House and Senate Judiciary Committee reports detail why: to simplify the statute.

Furthermore, this Court should adopt a broad reading of the statute based on agency and contract principles. Such principles have traditionally defined employer-employee relationships. Agency principles require employees to act in the interests of their employers, while contract law explicitly details the scope of the employer-employee relationship. Grounding the CFAA in both sources of law makes sense in light of their storied history dictating employer-employee relationships. If Congress had meant to alter such a classic employer-employee relationship, it would have said so explicitly in the statute.

Petitioner violated the CFAA when he accessed the CDC-Secure Database restrictions in contravention of both agency and contract principles, and used the information inappropriately. Petitioner lost authorization to the CDC-Secure Database the moment he intended to act against the interests of his employer Gant. She verbally denied Petitioner's request to publish confidential information regarding phyresis. She also moved him to another department that did not study phyresis. Further, Petitioner violated the explicit terms of the CDC-Secure Database.

While this Court should adopt a broad reading of the CFAA, it should not adopt a broad reading of the Fourth Amendment that adopts a mosaic approach. This Court has time and again adopted a sequential approach to the Fourth Amendment, in which the Court analyzes one

investigatory technique at a time. By adopting the mosaic approach, this Court runs the risk of overturning firmly entrenched precedent legalizing certain types of searches. This runs the risk of curbing too much police conduct to the detriment of society's safety. How will officers know when their investigation techniques go too far?

Even if this Court adopts the mosaic approach, the Government does not violate it. The approach is concerned with barring the Government from obtaining information that paints an intimate picture of a person's life. Here, the Government did not paint such a picture. Instead, it merely acquired a *sixteen-day* incomplete snapshot of *some* of Petitioner's activities. The Government does not know all of the Petitioner's medical conditions and prurient interests, or family, friends, hobbies, sports, religious affiliations, and marital status. Furthermore, even if the Government paints an intimate picture, society would find that picture a reasonably drawn one—for individuals, through social media and other technologies, regularly disclose such details.

For these aforementioned reasons, the Court should affirm both the Courts of Appeals' orders denying Petitioner's motion to dismiss CFAA claims and motion to suppress the fruits of the Government's investigation.

ARGUMENT

I. THE PLAIN WORDING AND LEGISLATIVE HISTORY OF THE COMPUTER FRAUD AND ABUSE ACT SUGGEST THAT CONGRESS, THROUGH THE PHRASE "WITHOUT AUTHORIZATION," INTENDED TO PROHIBIT THE UNAUTHORIZED USE OF A COMPUTER.

The Court of Appeals' decision denying Petitioner's motion to dismiss should be affirmed because the CFAA imposes a use restriction. The CFAA is the federal computer hacking statute. It was originally passed to combat digital crimes. There is currently a deep divide among the circuit courts for how to interpret the phrase "without authorization, " with courts reading the phrase broadly or narrowly. Under a broad reading, courts hold the CFAA prohibits individuals from adversely using their computers.[1] An employee may have initial authority to access the computer, but his or her subsequent *misuse* voids initial authority. This use restriction approach is grounded in two different sources: agency principles and contract law.

Not all courts adopt the broad reading of the statute. Instead, some read the statute narrowly to impose an access restriction.[2] Under such a restriction, an employee is liable only when he or she does not have initial *access* to the computer or information at hand. This approach is grounded in code-based theory, which states that if an individual physically hacks into a computer to use it, he or she is liable under the statute.

---

[1] The First, Fifth, Seventh, Eighth, and Eleventh Circuits have adopted a broad reading of the CFAA. *See, e.g.*, *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001); *United States v. John*, 597 F.3d 263 (5th Cir. 2010); *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *United States v. Teague*, 646 F.3d 1119 (8th Cir. 2011); *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010). The Third Circuit may have recently adopted the broad approach in an unpublished, non-precedential opinion. *See CollegeSource, Inc. v. AcademyOne, Inc.*, 597 F. App'x 116 (3d Cir. 2015).

[2] The Fourth, Sixth, and Ninth Circuits have adopted a narrow reading of the CFAA. *See, e.g.*, *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012); *Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am.*, 648 F.3d 295 (6th Cir. 2011); *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012).

A. The CFAA's Plain Language Prohibits the Unauthorized Use of a Computer.

The starting point for interpreting any statute is its plain text.[3] *Consumer Product Safety Commission et al. v. GTE Sylvania, Inc. et al.*, 447 U.S. 102 (1980) ("We begin with the familiar canon of statutory construction that the starting point for interpreting a statute is the language of the statute itself."). The CFAA states, "Whoever intentionally accesses a computer *without authorization* or *exceeds authorized access*" shall be liable. 18 U.S.C. § 1030(a)(2)(B) (2008) (emphasis added). The phrases "without authorization" and "exceeds authorized access" are synonymous—for one who exceeds authorized access on a computer operates without authorization on that computer. Both the Fourth and Seventh Circuits have expressly recognized this similarity. *See WEC Carolina Energy Solutions*, 687 F.3d at 204 ("the distinction between [the two phrases] is arguably minute"); *Citrin*, 440 F.3d at 420 ("the difference between [the two phrases] is paper thin.").

A closer look at the meaning of the words in both phrases marks their similarity. The definition of "exceed" is "to go beyond the bounds or limit of." *Exceed Definition*, *Random House Online*, www.dictionary.com (last visited January 8, 2016). The definition of "without" is "beyond the compass, limits, range, or scope of." *Without Definition*, *Random House Online*, www.dictionary.com (last visited January 8, 2016). The meaning and language of the definitions of both words is nearly identical, drawing the fateful conclusion that when an individual on a computer "exceeds" the scope of their authority, he or she is "without" authorization.

The CFAA's definition for "exceeds authorized access" also suggests the two phrases are identical. The CFAA defines "exceeds authorized access" as "to access a computer with

[3] Several courts have first looked to the text of the CFAA in order to determine its meaning. S*ee Pulte Homes Inc.*, 648 F.3d at 303 (court emphasizing that the starting point for interpreting the phrase without authorization is its "ordinary usage"); *WEC Carolina Energy* Solutions, 687 F.3d at 203–04 (court interpreting the CFAA using the plain meaning rule).

authorization and to use such access to obtain or alter information in the computer that the accessor is *not entitled so to obtain or alter*." 18 U.S.C. § 1030(e)(6) (2006) (emphasis added). When an employee is not entitled to obtain or alter information on a computer, he or she is without authorization with respect to that information. Not only are the phrases similar on their face, the definition of one phrase, explicitly provided for in the statute, makes the two identical.

Further, this definition of "exceeds authorized access" strongly suggests that the CFAA prohibits unauthorized use. In all the times Congress has amended the CFAA, it has never supplied a definition for the phrase "without authorization." But, that may be because the phrase "exceeds authorized access" is already defined. Its definition indicates that Congress adopted a use restriction. A close reading of the definition suggests that an individual who exceeds authorized access is one who initially had access to a computer, but because of *how* he or she used the computer, exceeded access. The definition imposes liability for an individual "who obtain[ed] or alter[ed]" information—or, in other words, misused a computer.

Petitioner may well invoke the mere surplusage canon of construction in arguing that the two phrases should not be construed identically. Under the canon, the Court must give effect to "every word of a statute wherever possible." *Ransom v. FIA Card Servs., N.A.*, 131 S. Ct. 716, 724 (2011). But, the surplus may have been for clarification purposes—Congress added the phrase "exceeds authorized access," and supplied it a definition, to further explain what "without authorization" meant. Further, Congress does not always engage in artful drafting. Neither does this Court. In granting certiorari to the third question on this appeal, the Court wrote, "[c]an potentially reasonable searches . . . be rendered unreasonable when considered *cumulatively or in the aggregate*." J.A. at 3 (emphasis added). This Court also writes surplus words.

B. The CFAA's Legislative History Prohibits the Unauthorized Use of a Computer.

The original language of the CFAA strongly suggests that Congress intended to prohibit the unauthorized use of a computer. Congress enacted the CFAA as a way to combat crimes committed through a computer, such as hacking. *See* Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, 98 Stat. 1837 (1984) (hereinafter "CCCA"). An individual was liable under the CCCA if he or she "knowingly access[ed] a computer without authorization, or having accessed a computer with authorization, *use[ed] the opportunity such access provides for purposes to which such authorization does not extend*." *Id.* (emphasis added). In other words, if an individual used a computer contrary to his or her employer's wishes, that individual was liable. The CCCA clearly prohibited unauthorized use.

While Congress deleted the phrase by passing the 1986 amendments to the CFAA, Congress did so only to simplify the statute's language. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (1986). The legislative history behind the amendments evinces Congress's intent to expand the CFAA's reach—not to curtail it. The amendments added three new types of computer crimes that were punishable. *Id.* What is more, a Senate Judiciary Committee report explained the purpose of the amendments: "*to expand* and amend 18 U.S.C. § 1030." *See* S. Rep. No. 99-432, at 3 (1986) (emphasis added). The House Judiciary Committee's explanation for why Congress substituted the phrase is even more persuasive:

> Section (2)(C) deletes the phrase 'or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend,' and substitutes 'or exceeds authorized access' in 18 U.S.C. 1030 (a)(1) (a)(2) . . . . *The purpose of this change is merely to clarify the language in existing law*.

H.R. Rep. No. 99-612 (1986) (emphasis added). Just like the House Judiciary Committee, the Senate Judiciary Committee explains that the original language was substituted for simplification purposes. *See* S. Rep. No. 99-432, at 9. The Senate Judiciary Committee explained:

> Section 2(c) substitutes the phrase 'exceeds authorized access' for the more cumbersome phrase in present 18 U.S.C. 1030(a)(1) and (a)(2), 'or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend.' *The Committee intends this phrase to simplify the language* . . . .

Id. (emphasis added). As such, even though Congress deleted the original language in the CCCA that explicitly adopted a use restriction, both the House and Senate Judiciary Committees explicitly detail why: to simplify the act's provisions.

Furthermore, the 1986 amendments to the CFAA were not the only amendments to expand the statute's reach—eight additional amendments did so as well.[4] For instance, the 1994 amendments added a civil provision, allowing victims of computer crimes the ability to recover civil damages against hackers. *See* Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-122, 108 Stat. 1796 (1994). The 1996 amendments expanded the types of computers that, if hacked, would impose liability on the hacker. 18 U.S.C. § 1030(a)(7) (1996). Through those amendments, not only would hacking "Federal interest computers" impose liability, hacking "protected computers," or any computer connected to the Internet, would too. As Professor Kerr notes, "the change in definition changed the scope of the statute dramatically." Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1561 (2010). Subsequent amendments expanded the reach of the statute—including the

[4] *See* U.S. Dep't of Justice, *Prosecuting Computer Crimes* 2 (2d ed. 2010), www.justice.gov ("As computer crimes continued to grow in sophistication and as prosecutors gained experience with the CFAA, the CFAA required further amending, which Congress did in 1988, 1989, 1990, 1994, 1996, 2001, 2002, and 2008.").

last major amendments in 2008.[5] Former Vice President Protection Act, Pub. L. No. 110-326, 122 Stat. 3560 (2008).

Consequently, the legislative history of the CFAA expressly contemplates that the statute forbids the unauthorized use on a computer. This legislative history serves a "confirmatory" role for the plain meaning of the statute. *See* 73 Am. Jur. 2d Statutes § 83 (2014). The original language of the CCCA explicitly punished those who misused a computer. Though the relevant language was deleted, subsequent legislative history indicates the change was *only* for simplification purposes. Both the House and Senate Judiciary Committee reports explicitly state the language was deleted to simplify the statute. Further, the overall history of the statute, in which Congress expanded it at least nine times over the course of more than a decade, strongly indicates that Congress intended the statute to be as broad as possible, and thereby prohibit unauthorized use.

C. Under the Facts of This Case, Petitioner Acted Without Authorization When He Misused the Computer

Petitioner clearly violated the CFAA when he misused the information he obtained from the CDC-Secure Database. He did so disclosing the information to the public through his website. Here, both employer Gant's express wishes and the CDC-Secure Database restrictions barred Petitioner from disclosing such information. Gant declined Petitioner's requests to divulge such information to the public at least two times—telling Petitioner to not publish the information. After Petitioner asked if he could a second time, Gant had had enough, and transferred Petitioner to a new department that dealt solely with Alzheimer's disease, not Phyresis. This transfer speaks just as many volumes as Gant's verbal admonishments. By

[5] Even the USA PATRIOT ACT, enacted in response to 9/11, expanded the reach of the CFAA. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

transferring Petitioner, Gant was implicitly removing all authority Petitioner had to investigate Phyresis. Besides violating the express and implied wishes of his employer, Petitioner violated the CDC-Secure Database restrictions that clearly barred disclosing information regarding Phyresis to the public. Petitioner knew well the content of the restrictions. First, he had to sign and agree to them every time he accessed the CDC-Secure database. Second, the text of the restrictions was easy to read: the font size was at least twelve-point font, and the entire restriction contained fewer than 100 words. Most telling, the font for the phrase "I understand these restrictions" was at least sixteen-point font. J.A. at 28–29. The Petitioner misused the information by breaching his contract and acting against the wishes of his employer.

II. THE AGENCY AND CONTRACT-BASED APPROACHES TO THE COMPUTER FRAUD AND ABUSE ACT SUPPORT THE NOTION THAT CONGRESS, THROUGH THE PHRASE "EXCEEDS AUTHORIZED ACCESS," INTENDED TO PROHIBIT THE UNAUTHORIZED USE OF A COMPUTER.

Agency and contract theory provide additional reasons why the Court should read the CFAA broadly.[6] Under agency theory, an individual must act for the sole interests of his or employer. An employee violates the CFAA when he or she uses a company computer in a way that is adverse to the employer's interests. There are many reasons why the CFAA should adopt the agency-based approach. First, Congress, through the statute's plain language, intended it. Second, the approach provides adequate notice to employees of what behavior is permissible.

[6] There is actually a third theory supporting a broad interpretation of the statute: norms-based theory. Professor Kerr explains that this theory will hold the user of a computer accountable under the statute if they use the computer "beyond the pale of accepted social practices" in the workplace. Orin S. Kerr, *Obama's Proposed Changes to the Computer Hacking Statute: A Deep Dive*, Volokh Conspiracy (Jan. 14, 2015), http://www.washingtonpost.com. The Fifth Circuit utilized norms-based theory to find liability. *United States v. Phillips*, 477 F.3d 215 (5th Cir. 2007). The court adopted found that the defendant violated "expected norms of intended use or the nature of the relationship established between the computer owner and the user." *Id.* at 219.

Agency theory has traditionally defined the employee-employer relationship. Accordingly, it makes sense for Congress to ground liability in such a time-honored principle.

Contract theory provides an additional reason why the CFAA imposes a use restriction. Under it, explicit contracts define the scope of the employer-employee relationship. The contract-based approach provides even more adequate notice to employees than the agency-based approach for what behavior is permissible. For one, many employer-employee relationships are already defined by contract. Further, a contract explicitly tells the employee what he or she can do on a computer. Thus, the Court should adopt the agency-based approach, the contract-based approach, or both, to read the CFAA broadly.

A. The Agency-Based Approach Provides a Persuasive Reason to Adopt the Broad Interpretation of the Phrase "Exceeds Authorized Access"

1. THE AGENCY-BASED APPROACH

The agency-based approach is grounded in the traditional principles of agency.[7] In an agency relationship, an employee owes a special duty of loyalty to the employer. That duty is to act primarily for the benefit of the employer.[8] As soon as the employee acts adversely to the employer's interest, the employee severs the agency relationship. As such, a computer user exceeds authorized access on a computer whenever that user uses the computer for purposes that do not further his or her employer's interest. Once the computer user acts adversely to his or her employer's interest, the agency relationship is terminated and the user loses authorization.

---

[7] Agency is the "fiduciary relation which results from the manifestation of consent by one person to another that the other shall act on his behalf and subject to his control, and consent by the other so to act." Restatement (Second) of Agency § 1 (1958). *See also* Restatement (Third) of Agency § 1.01 (2006).

[8] Restatement (Second) of Agency § 13 cmt. a (1958) ("The agreement to act on behalf of the principal causes the agent to be a fiduciary, that is, a person having a duty, created by his undertaking, to act primarily for the benefit of another in matters connected with his undertaking.").

The flagship case representing the agency-based approach is *Citrin*. 440 F.3d 418. In that case, the Seventh Circuit adopted an agency approach of the broad interpretation. The court held the defendant lost the authority to use his company's laptop when he decided to act adversely to his employer's interests. *Id.* at 421. By deleting valuable data that was stored on the company laptop, the defendant breached his agency relationship and no longer had authority to use the laptop. The court explains, "his authorization to access the laptop terminated when . . . he resolved to destroy files that incriminated himself and other files that were also the property of his employer, in violation of the duty of loyalty that agency law imposes on an employee." *Id.* The court directly cited agency principles to find the employee exceeded his authorized access.

2. THE REASONS WHY THE COURT SHOULD ADOPT THE AGENCY-BASED APPROACH

There are two reasons why this Court should adopt the agency-based approach. The first is that Congress intended to adopt the approach through the plain language of the CFAA. Under the definition of "exceeds authorized access," an individual is liable for obtaining or altering information he or she is not "*entitled so* to obtain or alter." *See* 18 U.S.C. § 1030(e)(6) (emphasis added). The definition of "entitle" is to "grant a legal right." *Entitle Definition*, *Black's Law Dictionary* (9th ed. 2010). As such, when an individual adversely uses a computer by obtaining or altering information, he or she loses entitlement on that computer. By losing entitlement, the agency relationship dissolves.

A second reason why the Court should adopt an agency-based approach is that it provides a predictable means of liability in the workplace. Specifically, the approach provides adequate notice to employees of when they violate the CFAA. The reason is that agency principles traditionally define employer-employee relationships. The CFAA merely preserves that

relationship—if Congress meant to disrupt the agency relationship, surely it would have said so explicitly in the statute.

3. UNDER THE FACTS OF THIS CASE, PETITIONER EXCEEDED HIS AUTHORIZED ACCESS WHEN HE VIOLATED HIS AGENCY RELATIONSHIP

Petitioner is liable under the agency-based approach for misusing information. Just like the defendant in *Citrin* who acted against his employer's wishes by destroying computer files, here Petitioner acted against his employer's wishes when he disclosed confidential information to the public. Specifically, Petitioner exceeded authorized access when he disclosed information regarding "the phyresis crisis" to the public through his website. Circumstantial evidence all but suggests Petitioner violated the wishes of his employer. On at least two occasions, Gant expressly denied Petitioner's request to divulge such information. Further, after Petitioner was denied a second time, Gant transferred him to another department, one that did not deal with phyresis whatsoever. This act suggests Gant did not want Petitioner dealing with the disease. Petitioner exceeding authorized access when he violated his agency relationship.

B. The Contract-Based Approach Provides an Additional Persuasive Reason to Adopt the Broad Interpretation of the Phrase "Exceeds Authorized Access"

1. THE CONTRACT-BASED APPROACH

Besides the agency-based approach, the contract-based approach provides an additional reason for why the Court should adopt the broad interpretation of the CFAA. Contract theory "finds its roots in contract law, focusing on the contractual relationship between the parties." Garrett Urban, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52 Wm. & Mary L. Rev. 1369, 1388 (2011). It declares a contract between an employer and employee

sets the grounds for how the user will use the computer. If the user violates those grounds, they violate the contract, in turn violating the statute. *Id.*

The flagship case representing the contract-based approach is *EF Cultural Travel BV*, 274 F.3d at 577. The case stands for the proposition that using a computer in violation of a contractual agreement constitutes exceeding authorized access. In that case, the defendant created a "scraper" computer software program that systematically gleaned prices on EF Cultural Travel's website. *Id.* at 579. This would help his new company, Explorica, undercut his old company's prices. The court focused much of its attention on the contract agreement the defendant had previously signed with EF Cultural Travel. The defendant promised "to maintain in strict confidence and not to disclose to any third party . . . any Confidential or Proprietary Information . . . for Employee's own benefit or for the benefit of any other person or business entity other than EF." *Id.* at 582. The defendant breached the contract, and thus violated the CFAA, when he used the scraper to analyze tour prices and thus obtain proprietary information. *Id.* at 583–84.

2. THE REASONS WHY THE COURT SHOULD ADOPT THE AGENCY-BASED APPROACH

There are several reasons why the contract-based approach is another appealing theory for which to base liability under the CFAA. First, even more so than agency theory, a contract-based approach adequately informs the employee of what behavior is permissible and impermissible. Employees must sign a written document, either an employment agreement or the terms and conditions that expressly define permissible conduct on a computer. There is sufficient notice through these explicit directions. Furthermore, similar to an agency relationship, employee-employer relationships are already usually defined by contract. Employees should not be surprised that the CFAA simply relies on such contract principles to

impose liability. Relatedly, an additional benefit of relying on this approach is that if there is no contract, the employee will not be liable. Consequently, this approach compels employers to give their employees notice of what behavior is allowed on company computers.

3. UNDER THE FACTS OF THIS CASE, PETITIONER EXCEEDED AUTHORIZED ACCESS WHEN HE VIOLATED HIS CONTRACT

Petitioner clearly violated a contract in this case, and, as such, should be liable under the contract-based approach. Every time Petitioner logged on to the CDC-Secure Database, he had to agree to use restrictions. The restrictions were clear: "All employees accessing the CDC-Secure system certify that they will not use the CDC database for the following prohibited activities . . . ." J.A. at 28–29. Following that text were a list of two proscribed activities, one of which was "Distributing or copying materials for the benefit or use of individuals not expressly authorized by the Centers for Disease Control . . . ." *Id.* Just like the defendant in *EF Cultural Travel BV* who explicitly violated the confidentiality agreement, Petitioner here violated explicit restrictions when he took information from the database regarding phyresis, and distributed it to the public through his website.

III. PETITIONER'S MOTION TO SUPPRESS WAS CORRECTLY DENIED BECAUSE THE GOVERNMENT'S ACTIONS WERE INDIVIDUALLY CONSTITUTIONAL, THE MOSAIC APPROACH IS AN IMPERMISSIBLE ANALYSIS OF FOURTH AMENDMENT PROTECTIONS, AND, EVEN IF IT IS APPLIED IN THIS CASE, THE GOVERNMENT'S ACTIONS DO NOT VIOLATE A REASONABLE EXPECTATION OF PRIVACY.

The Court of Appeal's decision should be affirmed, thereby reversing the grant of Petitioner's motion to suppress evidence. The court correctly rejected the mosaic approach to the Fourth Amendment because potentially reasonable government action cannot be rendered an "unreasonable search" under the Fourth Amendment when considered cumulatively or in the aggregate. The mosaic application of the Fourth Amendment is an impermissible and misguided reading that would require the Court to consider *all* of the government's actions in a specific

case, and evaluate them under the *Katz* two-prong privacy test—instead of each individual investigatory technique. Applying such an aggregate view would contravene decades' worth of precedent requiring courts to assess discrete government individually. This approach is sometimes referred to as the "sequential" approach.[9]

"The Fourth Amendment provides in relevant part that '[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.'" *United States v. Jones*, 132 S. Ct. 945, 949 (2012) (quoting U.S. Const. amend. IV). The reach of the Fourth Amendment does not "turn upon the presence or absence of any physical intrusion into any given enclosure," *Katz v. United States*, 389 U.S. 347, 353 (1967), but rather there may be a violation where there is an intrusion upon a "constitutionally protected reasonable expectation of privacy."[10] *Id.* at 360 (Harlan, J., concurring). Analyzing whether government action violates an individual's Fourth Amendment rights requires answering two questions: (1) "whether the individual, by his conduct, has 'exhibited an actual (subjective) expectation of privacy,'" and (2) "whether the individual's subjective expectation of privacy is 'one that society is prepared to recognize as reasonable.'" *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

The sequential approach is the traditional Fourth Amendment analysis under which courts analyze each government action separately in their chronological sequence to determine whether each action constitutes a "search". By considering government actions in the aggregate rather than individually, the mosaic approach would render otherwise permissible individual government action under the Fourth Amendment an unconstitutional search—directly

---

[9] *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311, 315 (2012).

[10] The Court recently articulated that *Katz* did not replace the traditional trespass understanding of the Fourth Amendment, but rather added to it. *Jones*, 132 S. Ct. at 952.

contradicting numerous decisions of this Court that hold individual techniques constitutional. This would lead to an unworkable standard, forcing both lower courts and government actors alike to guess what conduct, individually or in the aggregate, is constitutional. Further, this uncertainty would undermine the purpose of the exclusionary rule—to deter future violations—because if government actors cannot reliably ascertain what conduct is unconstitutional then a court excluding evidence would not have any effect on their actions.

The first part of this section argues that the Court should not adopt the mosaic approach because: (1) the Court effectively utilized the sequential approach for decades, and there is no societal need for this new analysis; (2) adopting the mosaic approach would invalidate numerous government actions that are already constitutional; (3) the mosaic approach would be unworkable for lower courts that would have to re-answer a plethora of questions that have been decided in the decades since *Katz*, in addition to novel questions arising from the approach; and (4) the approach would undermine the purpose of the exclusionary rule, deterrence, leaving aggrieved defendants without an effective remedy. The second part of this section argues that even if the Court does choose to adopt the mosaic approach, the Government's investigatory techniques in this case do not violate Petitioner's reasonable expectations of privacy when considered cumulatively. The information obtained by the Government does not paint a sufficiently intimate picture of Petitioner's life.

A. This Court Should Not Adopt the Mosaic Approach

1. The Supreme Court Has Successfully Utilized the Sequential Approach to Defend Fourth Amendment Rights Time and Again, and There Is No Contemporary Need to Change the Nature of the Analysis.

i. Maynard, Jones, and the Mosaic Approach

The mosaic approach has been expressed in three different opinions dealing with the same case. First, the D.C. Circuit applied an aggregate theory in *United States v. Maynard*, 615

F.3d 544 (D.C. Cir. 2010). In *Maynard*, the officers attached a GPS tracking device to the defendant's vehicle outside the scope of an expired warrant. The device was monitored for almost a month, continuously tracking the defendant's movements. Judge Ginsburg, writing for the majority, considered whether the defendant's movements *as a whole* were exposed to the public, rather than simply the movements of one journey. The court held that "[t]he whole of one's movements over the course of a month is not constructively exposed to the public because … that whole reveals far more than the individual movements it comprises." *Id.* at 561–62. Therefore, considered in the aggregate, the government's surveillance constituted a search.

In *Jones*, on appeal from the *Maynard* decision, the Court decided the case on trespass grounds, holding the officer's physical intrusion upon the space of the vehicle in order to attach the tracking device an unconstitutional search. However, Justices Sotomayor and Alito wrote two separate concurrences expressing theories that a reasonable expectation of privacy should be extended to consider the aggregate of government action.

Justice Sotomayor's concurrence focused on the possibility that GPS tracking enables the government to "generate[] a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring). Further, she advocated for a test that asks "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on." *Id.* at 956 (Sotomayor, J., concurring).

Justice Alito's concurrence, on the other hand, was concerned that the government could "secretly monitor and catalogue every single movement of an individual's car for a very long period." *Id.* at 964 (Alito, J., concurring). He also discussed whether the Court should vary

standards of constitutionality based on the severity of the offense: "[w]e also need not consider whether prolonged GPS monitoring in the context of investigations involving extraordinary offenses would similarly intrude on a constitutionally protected sphere of privacy." *Id.*

ii. The Sequential Approach

This Court has always utilized a sequential approach to analyzing whether Governmental investigatory techniques constitute a physical trespass under *Jones* or violate an individual's reasonable expectation of privacy under the *Katz* two-part analysis. Never has the Court combined two or more investigatory techniques and analyzed them in unison. As Professor Orin S. Kerr explains, courts utilizing the sequential approach analyze whether a search occurred through a "frame-by-frame dissection of the scene." Kerr, 111 Mich L. Rev. at 316. Essentially, the court takes a "snapshot of the act and assesses it in isolation." *Id.* at 315. In other words, courts analyze one individual investigatory technique at a time to determine whether a Fourth Amendment violation has occurred. The Court in *Terry v. Ohio* made this notion clear, when it articulated that the Court assesses "the reasonableness in all the circumstances of the *particular* governmental invasion of a citizen's personal security." 392 U.S. 1, 18 (1968) (emphasis added).

Every significant Fourth Amendment case has utilized the sequential approach, analyzing one particular governmental investigation or method. In *Olmstead v. United States*, the Court reviewed the government's warrantless wiretapping of private phone calls. 277 U.S. 438 (1928). Although the wiretapping occurred over time, the singular act of placing the tap was the piece analyzed. *Id.* In *Miller v. United States*, the Court reviewed whether officers could break into a defendant's home without notice to seize evidence. 357 U.S. 301 (1957). In *Katz*, the Court reviewed the government's placing of an electronic eavesdropping device attached to the exterior of a phone booth that recorded defendant's conversations. 389 U.S. at 347. In *Terry*, the Court reviewed a police officer's patting down of a defendant's outer clothing. 392 U.S. at 1. In *Smith*

v. Maryland, the Court analyzed the installation of a pen register by a telephone company at police request that recorded the phone numbers dialed by the defendants. 442 U.S. at 735. In *New York v. Class*, the Court reviewed whether an officer could reach into a car's interior to move some papers in order to identify the vehicle identification number on the dashboard that was covered by the papers. 475 U.S. 106 (1986). In *California v. Ciraolo*, the Court assessed an officer's naked eye observation of a defendant's backyard from a private airplane. 476 U.S. 207 (1986). In *Jones*, the Court reviewed the government's installation of a GPS tracking device on the defendant's vehicle. 132 S. Ct. at 945.

These cases illustrate two simple principles of traditional Fourth Amendment analysis. First, courts look to the government activity that collected the information and determine whether that *particular action* violated the individual's rights. Second, courts only look at the discrete step of information collection or observation. These principles are contradicted by the mosaic approach.

iii. The Sequential Approach Effectively Protects Fourth Amendment Rights

The mosaic approach is not needed to protect liberties as new technologies emerge. Advocates for the mosaic theory claim that it is a necessary approach that will supposedly restore lost protections to individuals because of emerging technologies. Professor Kerr calls this supposed phenomenon "equilibrium-adjustment." Kerr, 111 Mich. L. Rev. at 315. Petitioner may argue that new technologies, like license plate scanners and drones, present novel ways for the government to intrude upon people's lives. However, current Fourth Amendment inquiries grounded in the sequential approach already sufficiently protect individuals' rights, while still offering latitude to adjust with changing technology and societal expectations of privacy.

First, there are already two analyses under the Fourth Amendment, the physical trespass test in *Jones* and the *Katz* reasonable expectation of privacy test, that sufficiently safeguard privacy. These tests have been employed for decades for a wide variety of once-new technologies, and illustrate that the Court's Fourth Amendment analysis does keep up with the times. For instance, the Court in *Jones* deemed a GPS tracker attached to a car as too intrusive, 132 S. Ct. at 945, and the Court in *Kyllo* held that use of a thermal imaging device unconstitutionally intruded upon the home. 533 U.S. 27, 34–35 (2001). Each time a new technology has been introduced, the Court has effectively enforced the protections of the Fourth Amendment utilizing current analyses. The mosaic approach would depart from a time-proven method of enforcing the Constitution's protection from unreasonable searches.

2. THE MOSAIC APPROACH WILL INVALIDATE FIRMLY ESTABLISHED, CONSTITUTIONAL INVESTIGATORY TECHNIQUES.

The Court has ruled in the almost fifty years since *Katz* on whether various specific situations allow for a reasonable expectation of privacy. These interpretations of Fourth Amendment protections would be rendered meaningless by applying the mosaic approach, because it does not only look to the government's conduct but also to the information the investigation yields. Adopting the mosaic approach would lead to cases where government actors perform long-held constitutional investigations, but because of the nature of the information such action yielded, the overall investigation would be held unconstitutional. To invalidate the Court's voluminous precedent on everything from visual observation to use of aerially deployed cameras would cause constitutional turmoil, which would transcend technologies and methods.

As the Court in *Jones* wrote, "Th[is] Court has to date not deviated from the understanding that mere visual observation does not constitute a search." 132 S. Ct. at 953. IN

the same spirit, the Court in *Katz* wrote, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." 389 U.S. at 351. These two principles are consensus black-letter Fourth Amendment law, understood as such for almost fifty years, if not longer. But, now, the mosaic approach threatens their validity. Sitting outside the subject of an investigation's home and visually observing him for some period of time might yield the type or quantity of information that allows the government to form an "intimate picture" of a person's life. *See Maynard*, 615 F.3d at 563. However, this type of government action has always been acceptable under the Fourth Amendment, as even the court in *Maynard* conceded. 615 F.3d at 565 ("Surveillance that reveals only what is already exposed to the public—such as a person's movements during a single journey—is not a search.").

The court in *Maynard* erred in addressing these concerns, because it placed too much emphasis on the duration of the surveillance at issue and the impracticalities of extended mobile visual surveillance. *See id.* at 565–66. Under the mosaic approach, sitting outside the subject's home may be found unconstitutional regardless of the duration, if the observations made about the subject are of a certain character. *See Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (explaining the potential "detail about her familial, political, professional, religious, and sexual associations"). While the court in *Maynard* was concerned about aggregation of movements over a month while the subject moved around town, similar insights into a person's private life may be gleaned from simply observing the subject's movements around the visible parts of the home and property. *See Maynard*, 615 F.3d at 561–62 (concerned that the "whole reveals far more than the individual movements it comprises," and that no single action "reveals the habits and patterns that mark the distinction between a day in the life and a way of life.").

If the logic of *Maynard* and the concurrences' in *Jones* is accepted, then the pole camera utilized by the Government in this case could be unconstitutional. Since the camera operated continuously outside of Petitioner's home for five days, the logic in *Maynard* would posit that a person would have a reasonable expectation of privacy in not having their movements around their home aggregated in such a manner. This conclusion not only contradicts this Court's precedent, but also what the parties and other court decisions in this very case have all agreed on: the individual constitutionality of the Government's methods. J.A. at 7–8, 23 (while contested at the trial level, the individual constitutionality of the methods employed is not an issue on appeal). It is arguably only because the visual surveillance of the home did not *yield* any intimate details of Petitioner's activities that its use is not contested here. However, when discerning the appropriate standard for protecting individuals' Fourth Amendment rights, whether the government was successful in obtaining information about the defendant should not be a factor in the analysis.

Unsuccessful government surveillance may nevertheless violate an individual's Fourth Amendment rights. Yet, the premise of the mosaic approach is that the government *has acquired* revealing information about the subject's life, therefore it is a violation of privacy. In this way, it essentially makes unconstitutional the otherwise constitutional means employed based upon its view of the end result. This makes it an impermissible, and unworkable, analysis of potential Fourth Amendment violations and should therefore be rejected.

3. THE MOSAIC APPROACH WILL PRESENT AN UNWORKABLE STANDARD FOR COURTS, REQUIRING THEM TO ANSWER NUMEROUS QUESTIONS THAT HAVE ALREADY BEEN SETTLED UNDER THE SEQUENTIAL APPROACH, AND REQUIRING THEM TO ANSWER DIFFICULT LINE-DRAWING QUESTIONS FOR WHAT CONDUCT IS PERMISSIBLE UNDER THE FOURTH AMENDMENT.

Adopting the mosaic approach would present an unworkable standard for the courts. It would invalidate decades' worth of precedent on various Fourth Amendment search issues, and

require courts to answer questions that the Court has taken more than fifty years to settle since employing the *Katz* two-part test—in addition to raising novel questions unique to the mosaic approach. Traditional Fourth Amendment analysis looks to the specific government conduct that collected the evidence at issue, whereas the mosaic approach takes into account the aggregation, the analysis, and the interpretation of information to form a picture of the subject's "private" life. In doing so, the approach considers the "ends" of the government investigation and observation, in addition to the "means." This raises unique questions relating to the type, scope, content, etc. of the information collected, analyzed, and/or aggregated that would constitute a Fourth Amendment violation.

Implementing the mosaic approach would require courts to first answer fundamental questions, because the theory itself still contains significant ambiguities. To start, courts must decide what standard to apply: the mosaic "approach" is subject to several competing interpretations. Between the court in *Maynard* and the two justices' concurrences in *Jones*, there are three different theories for how to view potential Fourth Amendment violations in the aggregate. Furthermore, none of the three represent a workable test in their current form. Therefore, as an initial question the courts would have to decide which theory to adopt, and only then be able to formulate the specific test to use.

Even if a test were to be promulgated, there are difficult questions to decide, which are made more complicated than traditional standards when considered in the aggregate. Given that the mosaic approach considers not the specific investigative technique, but the fruits of the investigation as a whole, courts would have to settle on what society's reasonable expectation is for police investigations. However, most average individuals do not have any experience with

police investigations. Therefore, there would be little to no "societal" basis upon which to form a reasonable expectation. *See* Kerr, 111 Mich. L. Rev. at 330.

Next, courts would have to settle on the scope of the investigatory process that applies: information gathering, analysis, or use. Traditionally, courts have only looked to the information gathering or acquisition to determine whether some action constituted a search, and the other two phases were thought to be beyond the scope of protections. However, the three mosaic-based opinions, by focusing on the potential for the government to "secretly monitor and catalog every single movement," *Jones*, 132 S. Ct. at 964 (Alito, J., concurring), of an individual over time and to revisit that data "more or less at will," *id.* at 956 (Sotomayor, J., concurring), open up the theory of Fourth Amendment protections extending beyond the information acquisition phase. Given that the Fourth Amendment only applies to state actions, *United States v. Jacobsen*, 466 U.S. 109 (1984), identifying which precise stage(s) the mosaic theory can be applied to is significant. If the government acquired information obtained by private surveillance, which did not as the government's agent in obtaining the information initially, then would simply creating a database of the information implicate the Fourth Amendment?

Since mosaic theory is concerned with the government aggregating information to learn intimate details about an individual's life, courts would have to decide on the duration and scale of the investigation necessary to violate the Fourth Amendment. Length of time of the investigation and the methods used (how many, what technology, etc.) are significant questions that have already been answered in various situations coming before this Court under the sequential approach. Further, duration may be considered an easier question, with the longer the time the more invasive it seems, but shorter investigations may still yield a "comprehensive record" of an individual's activities. *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).

As discussed above in Part II(A)(2), the mosaic approach places emphasis on the end result of government surveillance: the aggregation of information such that the government invades an individual's "privacy" by obtaining an intimate or comprehensive view of his life. This shift in focus changes how Fourth Amendment matters come before the court for review. Under the traditional sequential approach, a defendant could point to specific instances of invasive government activity for the court to analyze, and rule on whether the fruits of that investigative activity were excluded for trial. Under the mosaic approach, the government may intrude upon an individual's reasonable expectation of privacy, but if the investigation does not produce information contributing to a comprehensive record of the individual's life, then it would not be unconstitutional. The question left unanswered by proponents of the mosaic approach is the role of the penalty or remedy for Fourth Amendment violations: the exclusionary rule. *See* Part II(A)(4), *infra*. Further, in situations in which a defendant's rights have been violated in specific instances, but individually and/or in the aggregate there was not information giving rise to an intimate view of his life, what remedy is there? As the age-old maxim provides: *ubi jus ibi remedium*—for every wrong, the law provides a remedy. Stated another way, a right without a remedy is no right at all.

4. The Mosaic Approach Leaves Courts Without an Effective Remedy for Fourth Amendment Violations Because It Is Unworkable for Government Actors to Conform Their Conduct to an Uncertain Standard.

The outcome, or remedy, traditionally for a Fourth Amendment violation is a judicially created safeguard called the exclusionary rule. The purpose of the exclusionary rule is to deter similarly unconstitutional future government action. However, the mosaic approach undermines the exclusionary rule: because the approach creates uncertainty as to what government conduct

constitutes a Fourth Amendment violation. As such, there is no deterrent effect accomplished by the applying the rule to improperly obtained evidence under the mosaic approach.

The Fourth Amendment protects against unreasonable searches, but "contains no provision expressly precluding the use of evidence obtained in violation of its commands." *Arizona v. Evans*, 514 U.S. 1, 10 (1995). However, the courts over time have fashioned the rule to "forbid[] the use of improperly obtained evidence at trial." *Herring v. United States*, 555 U.S. 135, 139 (2009). "The [exclusionary] rule's sole purpose, we have repeatedly held, is to deter future Fourth Amendment violations." *Davis v. United States*, 131 S. Ct. 2419, 2426 (2011). In cases where suppressing evidence would not yield "appreciable deterrence," the exclusionary rule does not apply. *Herring*, 555 U.S. at 141; *Davis*, 131 S. Ct. at 2426–27. Courts balance the benefits of deterrence of potential future Fourth Amendment violations against the costs to society in excluding the evidence and possibly allowing a guilty defendant to go free. *Herring*, 555 U.S. at 141. "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.* at 144. "But when the police act with an objectively reasonable good-faith belief that their conduct is lawful . . . the deterrence rationale loses much of its force." *Davis*, 131 S. Ct. at 2427–28 (citations and quotation marks omitted).

In *Herring*, the Court held that an accidental record keeping error, which led to the warrantless arrest of the defendant, was not sufficient to apply the exclusionary rule. The officer's conduct "was not so objectively culpable as to require exclusion." 555 U.S. at 146. In *Davis*, the Court found that officers' investigation conducted in objectively reasonable reliance on binding judicial precedent was not subject to the exclusionary rule, because the only deterrent value would be to "discourage the officer from doing his duty." 131 S. Ct. at 2429.

Here, adopting the mosaic approach would render Fourth Amendment rights meaningless. *Ubi jus ibi remedium*: a right without remedy is no right at all. If this Court adopts the mosaic approach, then the exclusionary rule would be inapplicable in cases of potential Fourth Amendment violations, because there would be no deterrent value in the vast uncertainty that the mosaic approach creates, leaving defendants without an effective remedy to enforce their Fourth Amendment rights.

The mosaic approach, by focusing on the aggregation of information, or the ends of an investigation, creates uncertainty as to what specific conduct by the government would be a violation of an individual's Fourth Amendment rights. This, in turn, does not allow law enforcement and other government actors to conform their investigatory conduct to an understanding of permissible investigatory methods. Therefore, there would be no deterrent value in applying the exclusionary rule, and the balance of interests would weigh in favor of the cost to society if guilty defendants go free. Such a balance means that it would be inappropriate to apply the exclusionary rule.

Further, if the exclusionary rule could not be applied in cases of Fourth Amendment violations to exclude improperly obtained evidence at trial, then what remedy would there be for government invasions of privacy? One option is for a defendant to sue the government and/or individual government actors responsible for the violations. William J. Stuntz, *Warrants and Fourth Amendment Remedies*, 77 Va. L. Rev. 881, 900–09 (1991). However, although civil suits for damages may be brought against government actors for rights violations, doctrines such as qualified immunity may limit their effectiveness, both in relieving the aggrieved defendant and also in deterring future conduct. Orin S. Kerr, *Fourth Amendment Remedies and Development of*

the Law: A Comment on Camreta v. Greene *and* Davis v. United States, 2011 Cato Sup. Ct. Rev. 237, 241–42 (2011).

Adopting the mosaic approach would eliminate the deterrent effect of the exclusionary rule, rendering it inapplicable, and thereby leaving defendants in cases implicating Fourth Amendment violations without an effective remedy to enforce their rights.

B. Even if This Court Does Adopt the Mosaic Approach, the Government's Actions in This Case Are Not Rendered Unreasonable Under the Fourth Amendment When Considered Cumulatively or in the Aggregate.

Even if the Supreme Court does adopt the mosaic approach, the Government's investigatory techniques do not violate Petitioner's Fourth Amendment rights. Under the mosaic approach, prolonged governmental surveillance that paints an intimate picture of an individual's life violates that individual's expectation of privacy under the Fourth Amendment. According to Justice Sotomayor, the purpose behind the mosaic approach is to curb "too permeating police surveillance." *Jones*, 132 S. Ct. at 956. Further, the policy behind why intrusive technologies, such as GPS devices, must be curbed by adoption of the mosaic approach lies in the notion that new technologies "alter the relationship between citizen and government in a way that is inimical to democratic society." *Id.* at 956 (citing *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring). Advocates of the mosaic approach believe that it is a necessary reading of the Fourth Amendment in an age where new technologies are more intrusive than ever, however their fears are unfounded when viewed in light of the history of the Court's application of the *Katz* test to adequately deal with emerging surveillance technologies.

1. The Mosaic Approach Is Grounded in the Notion That Prolonged Investigations Paint an Intimate Picture of an Individual's Life.

Under the mosaic approach, the government cannot engage in prolonged surveillance that paints an intimate picture of an individual's life. *Maynard*, 615 F.3d at 563; *Jones*, 132 S. Ct. at

955 (Sotomayor, J., concurring). In *Maynard*, the exemplar case for applying the mosaic approach, the defendant argued that the district court erred in admitting evidence acquired by the government's warrantless use of a GPS device. 615 F.3d at 549. To follow his movements, the government attached a GPS tracker to the defendant's vehicle, and tracked his movements continuously for twenty-eight days—amassing approximately 672 hours' worth of location information. The court of appeals held that such tracking was a search. The court solely focused on the second prong of the *Katz* privacy test, asking if society would find that Jones had a reasonable expectation of privacy in the totality of his movements on public roads. *Id.* at 558.

The court in *Maynard* answered in the affirmative, basing the central part of its holding on the notion that continuous surveillance for a prolonged period of time painted too intimate a picture of Jones's life. *Id.* at 563. The court explained how the mosaic approach rendered the GPS surveillance unconstitutional: "what may seem trivial to the uninformed, may appear of great moment to one who as a broad view of the scene." *Id.* at 562 (citation and quotation marks omitted). The mosaic theory is grounded in the notion that the government, through various pieces of information connected to a person, *may, over time, come to know that person too well*.[11] Further, "[a] person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, *but all such facts*." *Id.* (emphasis added). *See also State v. Jackson*, 76 P.3d 217, 224 (Wa. 2003) (en banc) ("In this age, vehicles are used to take people to a vast number of places that can reveal preferences, alignments, associations, personal ails and

[11] "Many nonsearches packaged together as an entity *became* a search because the individual pieces of the puzzle that seemed small in isolation could be assembled together like a mosaic to reveal the full picture of a person's life." Kerr, 111 Mich. L. Rev. at 325.

foibles. The GPS tracking devices record all of these travels, can thus can provide a detailed picture of one's life.").

Justice Sotomayor's concurrence in *Jones* echoes the notion that a violation of the Fourth Amendment under the mosaic approach depends on whether the government's prolonged surveillance paints an intimate picture of an individual's life. She writes, "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflect a wealth of detail about her familial, political, professional, religious, and sexual associations." *Jones*, 132 S. Ct. at 955.

2. HERE, THE GOVERNMENT'S ACTIONS DO NOT PAINT A COMPREHENSIVE OR INTIMATE PICTURE OF PETITIONER'S LIFE SUFFICIENT TO CONSTITUTE A SEARCH.

The Government did not violate Petitioner's Fourth Amendment rights under the mosaic approach because its combined investigatory techniques do not paint an intimate picture of Petitioner's life.

i. The Government Did Not Acquire Sufficiently Intimate or Comprehensive Information.

To begin, the Government did not collect information that painted a sufficiently intimate picture of Petitioner's life. A careful consideration of the all information obtained, and not obtained, by the Government's investigations reveals a sparse record of Petitioner's activities. From the five-day video surveillance, the Government monitored Petitioner's comings and goings, his unidentified food and package deliveries, some of his eating habits, and some of his visitors. From the following ten day use of license plate scanners, the Government learned that Petitioner drove on the state roadways three times, visited gentlemen's clubs three times, visited a grocery store twice, visited a psychiatrist's office twice, visited a urologist's office twice, and visited a nearby restaurant once. Finally, from the twenty-minute use of a video-surveillance

drone, the Government learned that Petitioner was in his backyard talking to the co-conspirator. The information gleamed does not paint an intimate picture of Petitioner's life, nor even a comprehensive record of two weeks' worth of his activities. For one, virtually all Americans enter and leave their homes, go to nearby restaurants, shop at local grocery stores, use state roadways, have people over at their homes, and order package and food deliveries. This information is not intimate or private, but the data points convey only that information a person already routinely conveys to the public eye.

The Government concedes that some information it obtained appears intimate on its face: Petitioner's visits to doctors and his apparent trips to gentlemen's clubs. However, even then, such information only offers a glimpse of two potentially private activities. Petitioner may have needed to go to the urologist and psychiatrist, but merely going there does not reveal the purpose thereof, or what occurred. Similarly, the scans of Petitioner's license plate adjacent to gentlemen's clubs do not indicate his personal preferences or orientations, but the simple fact of his vehicle's location at a given point in time.

Next, consider the crux of the information obtained: possible eating habits, medical facility visits, and various locations passed by. Notably absent from the Government's mere sixteen-day investigation is information regarding the totality of Petitioner's personal and private life. At some point, government investigations can form a record of a person's life that is too comprehensive or intimate. However, with all of the unknowns and gaps in the Government's investigation here that point was not reached in this case.

ii. The Duration of the Government's Investigation was Insufficient to Implicate Mosaic Theory Fourth Amendment Concerns.

The Government did not carry on its investigation for such duration so as to paint a comprehensive picture of Petitioner's life. It is impossible to know the intimate details about a

person's life from only observing their sporadic and momentary actions for sixteen days. It is unlikely that even direct contact with a person for that allotted time, continuously, would enable one to sufficiently know the individual completely. As such, the Government's investigation did not engage in the prolonged surveillance necessary of the kind in *Maynard* and *Jones*.

In *Maynard*, the court held that police surveillance using a GPS device for twenty-four hours a day for twenty-eight days was enough time to paint an intimate picture of a person's life. Justice Alito, in his concurrence in *Jones*, agreed, stating that a comprehensive record was formed before the four-week mark. However, assuming, for the sake of argument, Justice Alito's view of an impermissible duration, the Government in the present case did not monitor Petitioner's movements for a sufficient period of time that would give rise to a Fourth Amendment violation in the aggregate. Here, the investigation lasted a total of sixteen days: five days of electronic surveillance of the front of Petitioner's home, ten days of sporadic location spotting of the location of Petitioner's car, one additional day of visual surveillance of the back of Petitioner's home, and twenty minutes of aerial surveillance via a drone at altitude above the backyard of Petitioner's home. Sixteen days is only slightly more than half of the twenty-eight days that the court in *Maynard* found to be sufficiently invasive. More specifically, in *Maynard*, the police acquired exactly 672 hours' worth of surveillance regarding the defendant's movements in his car. Here, the police acquired only 145 hours' worth of surveillance (either electronic or visual) when Petitioner was at his home, and arguably one additional hour if the near instantaneous license plate scanner hits and twenty minute drone surveillance are taken into account. Therefore, the actual duration of surveillance here is distinguishable from the surveillance in *Maynard* and *Jones*.

Further, the nature of the surveillance in this case is less intrusive than the surveillance in *Maynard*. A GPS tracking device is undoubtedly a more invasive and efficient means for finding intimate details about a person's life than video surveillance, license plate scanners, visual observation, and brief aerial surveillance. Indeed, the video surveillance at issue proved useless to the Government, and they abandoned the approach. The subsequent use of license plate scanners only sporadically gave the Government the momentary location of Petitioner's vehicle, possibly not even of Petitioner himself. The aerial surveillance identified Petitioner's location on his property, but only for twenty minutes. None of these approaches, even in unison, offer twenty-four hour continuous surveillance of the kind used in *Jones* through the use of a GPS tracking device. Accordingly, the Government's sixteen-day investigation utilizing these means does not implicate Fourth Amendment protection, even when considered cumulatively.

3. EVEN IF THE MOSAIC APPROACH HERE DOES PROVIDE AN INTIMATE PICTURE OF PETITIONER'S LIFE, SOCIETY HAS NO REASONABLE EXPECTATION OF PRIVACY IN LOCATION DATA IN TODAY'S INCREASINGLY ADVANCED TECHNOLOGICAL WORLD.

Even if this Court finds that the Government did obtain an intimate picture of Petitioner's life, such a view was not a violation of a reasonable expectation of privacy under the Fourth Amendment. In today's world, society would find that Petitioner does not have a reasonable expectation of privacy in his location data. A plethora of recent technological changes—which society has implicitly and explicitly accepted—has eroded the privacy expectations individuals might reasonably assert in their location data.

Under the mosaic approach, the central inquiry is whether society would find that the Government investigation violated an individual's reasonable expectation of privacy. Justice Sotomayor explains, "I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at

will, their political and religious beliefs, sexual habits, and so on." *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring). Further, she believes that people "would [not] accept without complaint the warrantless disclosure to the Government" of their intimate life facts. *Id.*

However, society's understanding of reasonable expectations of privacy can narrow over time as people trade privacy for comfort or advances in technology. Justice Alito notes this, explaining, "technology can change those [society's] expectations. Dramatic technological change may . . . ultimately produce significant changes in popular attitudes. New technology may provide increased convenience at the expense of privacy, and many people find the tradeoff worthwhile." *Id.* at 962 (Alito, J., concurring).

Society does not view an individual's expectation of privacy in his or her location data as reasonable. *United States v. Graham*, 846 F. Supp. 2d 384 (D. Md. 2012). In *Graham*, the court held that the government did not violate the defendants' expectations of privacy when it collected their cell phone location data without a warrant. The government collected approximately 21,863 cell site location data points of the defendants over a course of 235 days. The defendants argued that such "twenty-four hour dragnet surveillance" allowed the government "to paint an intimate picture of the Defendants' whereabouts over an extensive period of time." Still, the court upheld the government's investigation for two reasons. First, Congress in the Stored Communications Act did not require the government to obtain a warrant for access to such information.[12] To the court, this meant that Congress all but stated that individuals do not have a privacy interest in their location data. Second, the court found that

[12] Congress instead required "specific and articulable facts" for why the government needs the cell phone location site data—a standard lower than the probable cause one for a warrant. Accordingly, such a lower standard strongly suggests that society does not believe that individuals have a reasonable expectation of privacy.

people who voluntarily conveyed their cell phone location data to their cellular providers "relinquish any expectation of privacy over those records."

Even though the Government's investigation may paint an intimate portrait of Petitioner's life, society will find that, in general, people have no reasonable expectations in such intimate data that is accumulated through their locations. As Justice Alito explained, people using new technologies sacrifice privacy rights for comforts. With the advent of significant technological changes, perhaps the time has come when society loses all expectations of privacy in individuals' location data—and thereby the potentially intimate facts derived from public movements. In this ever-connected world, people are constantly advertising their locations through Facebook (which allows users to Check-In at public places), Fitbit watches (in which users agree to send location recording data to the company), and iPhones (in which users also agree to send location recording data to the company).

Assuming that society holds the view that people generally have a right to intimate details acquired from their locations, Petitioner in this case still does not have a reasonable expectation of privacy thereof because he disclosed the information. In *Graham*, the court held that 21,863 cell site location data points, over the course of 235 days, did not violate the defendants' reasonable expectations of privacy—even when some of the location points tracked the defendants directly to their homes. Part of the court's reasoning was based on an act passed by Congress, in which Congress found that individuals do not have a reasonable expectation of privacy in their cell phone location data. Here, the Government has drastically fewer data points—only twelve locations of where Petitioner was traveling over the course of ten days. Further, none of the hits immediately tracked Petitioner to his home. Congress's reasoning in the realm of cell phones can be translated to Petitioner's driving a car in public: there is no

reasonable expectation of privacy in aggregating movements along public roadways. Moreover, as the court noted, the defendants in *Graham* voluntarily disclosed their location information to their cell phone providers, thereby relinquishing any expectation of location privacy. Similarly here, Petitioner relinquishes the privacy of his location when he travels in public, by voluntarily disclosing his person, vehicle, license plate, etc. that may be aggregated.

CONCLUSION

For the aforementioned reasons, the Government respectfully requests that the Court affirm both the orders of the Court of Appeals, denying Petitioner's motion to dismiss and to suppress the evidence.

Respectfully submitted,

/s/_____
Team 14
Counsel for Respondent
January 11, 2016