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 the Petitioner

Team No. 7

Counsel for the Petitioner

QUESTIONS PRESENTED

1. Does the term "without authorization" in the Computer Fraud and Abuse Act contemplate only unauthorized access, or does it also extend to include unauthorized use?

2. Can the term "exceeds authorized access" in the Computer Fraud and Abuse Act determine an employee has exceeded his or her authorized access by a resort to agency principles?

3. Can potentially reasonable searches under the Fourth Amendment be rendered unreasonable when considered cumulatively or in the aggregate?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Constitutional Provisions

OPINIONS BELOW

The opinion of the United States Court of Appeals for the Fourteenth Circuit is unreported but described in the Joint Appendix at J.A. 4-12. The United States District Court for the District of Greyhawk's opinion is also unreported but described in the Joint Appendix at J.A. 13-27.

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.

18 U.S.C. § 1030(a)(2)(B)

Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--information from any department or agency of the United States.

STATEMENT OF THE CASE

For twenty years, Gerrard Leomund worked for the Centers for Disease Control ("CDC") as a prized statistician, predicting the spread of infectious diseases across the country. Joint Appendix ("J.A.") at 13. Leomund held a known belief that all CDC data, including preliminary data, should be reported for the benefit of the public. J.A. at 13. Leomund earned a promotion to the position of Assistant Content Director/Disease Project Analyst in the Public Reports Division of the CDC. J.A. at 13.

Upon his promotion, Leomund received access to CDC-Secure, the protected software database where all CDC data is kept. J.A. at 14. Every time an employee accesses the software database, he or she must read and agree to the restrictions upon logging into database. J.A. at 14. These restrictions were also explained to all members of Leomund's division at the CDC. J.A. at 14.

In January 2013, the CDC began cataloging information regarding the spread of a new foreign pathogen, Phyresis. J.A. at 14. In the three months that followed, hospitals reported dozens of Phyresis infections that presented with terrible symptoms, including sepsis, muscle loss, delirium, and necrosis. J.A. at 14. On April 5, 2013, out of concern for the public, Leomund made a formal written request to his supervisor that the Phyresis data be publically released. J.A. at 14. Leomund's supervisor, Dana Gant, disagreed, reprimanded Leomund for his request, and told him to continue his analysis of the disease. J.A. at 14.

Leomund complied with his supervisor's request until, about a month later, he noticed a pattern in the Phyresis data that indicated a potential for an exponentially expansive outbreak of infections. J.A. at 14. On May 10, 2013, Leomund again submitted a formal request to Gant that this data be released to the public, and again Gant told him to continue his analysis and to stop objecting to withholding of information from the public. J.A. at 14. Shortly thereafter, Gant followed-up with Leomund via e-mail, stating that Leomund would be transferred to a different division at the CDC where he would be analyzing Alzheimer's disease in American citizens. J.A. at 14. Though he transferred divisions, Leomund retained access to CDC-Secure. J.A. at 14. Leomund was never informed by Gant that his new position limited his CDC-Secure access in any way.

On May 14, 2013, Gant viewed a news report on Phyresis, which referenced the website www.PhyresisGate.com. J.A. at 14. Gant found that the website contained information about the illness which came from the CDC-Secure database. J.A. at 14. Gant suspected this information came from Leomund, but could not confirm it. J.A. at 14. On Friday, May 17, 2013, Gant viewed another report on the Phyresis outbreak, which disclosed confidential information that was only available in the CDC-Secure database. J.A. at 14. Gant was informed by a member of the CDC's Information Technology department that, shortly after his transfer, Leomund's credentials had been used to access the Phyresis data. J.A. at 14. Gant then began the formal process for terminating Leomund, who did not return to work the following Monday, May 20th. J.A. at 14.

On Friday, May 24, 2013, a CDC employee informed Gant that www.PhyresisGate.com had been updated with data, but that the data had not been collected until Wednesday, May 22, 2013, after Leomund had stopped reporting to work. J.A. at 15. Gant reported her suspicions about Leomund's involvement in the unauthorized disclosures to the FBI, and subsequently federal agents came to the CDC and interviewed Gant about the agency's data collection and analysis. J.A. at 15. Gant described a three step process: first, a Pathogen Analyst collects data and processes the information into a spreadsheet; next, a Disease Topography Specialist uses the information to create a three dimensional contoured mapping using CDC custom printers; and finally, a Disease Projection Analyst, such as Leomund, creates an expected outbreak schedule based in part on the specialized maps. J.A. at 15. The expected outbreak schedule is then used to formulate CDC policy initiatives and countermeasures to fight the disease. J.A. at 15.

On May 27, 2013, federal law enforcement from the FBI set up a camera on a telephone pole outside of Leomund's home in Long Island, New York. J.A. at 15. The FBI had access to uninterrupted video stream from the camera to their headquarters in midtown Manhattan for five

continuous days. J.A. at 15. On Thursday, May 30, 2013, FBI agents were informed that www.PhyresisGate.com had been updated with confidential information from CDC-Secure, which led them to suspect Leomund was meeting with CDC employees outside of his home when he would leave for long periods of time. J.A. at 15.

On June 1, 2013, the FBI began running Leomund's license plate and vehicle information into a federal and state license plate scanner. J.A. at 15. The database is used by police officers who have car scanners which capture the license plate numbers of all passing vehicles. J.A. at 15. The scanner is typically used to determine if passing drivers have outstanding arrest warrants. J.A. at 15. Over ten days, the FBI picked up twelve "hits" on Leomund's car, including personal trips to the urologist, psychiatrist, and a number of gentlemen's clubs in the area. J.A. at 15. One match occurred while Leomund was driving on a state roadway near his home, which led a dispatched local police officer, Diego Armando, to notice a second entrance to Leomund's property. J.A. at 15. Officer Armando then staked out that entrance of Leomund's home during the days that followed. J.A. at 15.

On June 12, 2013, Officer Armando informed the FBI's Manhattan office that a vehicle not owned by Leomund had entered his property. J.A. at 16. Based on that information, the FBI and local police precinct surveyed inside of Leomund's property with an unmanned quadrocopter drone equipped with a digital camera. J.A. at 16. For twenty minutes, the FBI received live video feed straight from the camera to their Manhattan office of Leomund's property from 400 feet above. J.A. at 16. "Zooming in" on the camera, FBI investigators saw Leomund and Mike Edgeworth, a CDC Disease Topography Specialist, viewing one of the CDC's specialty contoured disease maps in Leomund's backyard. J.A. at 16.

The local police and FBI used this evidence to obtain an arrest warrant, and shortly thereafter took Leomund and Edgeworth into custody. J.A. at 16. While in custody, Leomund confessed to accessing the Phyresis files after his transfer, creating www.PhyresisGate.com, and working with Edgeworth to update the site after he had been terminated. J.A. at 16.

The District Court correctly held that Leomund had not violated the Computer Fraud and Abuse Act ("CFAA"), interpreting Leomund to not only have had authorization to access the Phyresis files, but also not to have exceeded such authorization in doing so. J.A. at 16-22. Additionally, the District Court held that the police and FBI's surveillance in the aggregate constituted an unreasonable and unconstitutional search of Leomund. J.A. at 22-27. The District Court granted Leomund's motion to dismiss and suppressed all evidence against him. J.A. at 27. The Court of Appeals for the Fourteenth Circuit rejected the District Court's holdings, and found Leomund guilty of violating the statute and the two and half weeks of constant surveillance permissible. J.A. at 5-12. The Supreme Court of the United States granted Leomund's writ of certiorari, and this case now sits before the Court. J.A. at 3.

SUMMARY OF THE ARGUMENT

Petitioner, Gerrard Leomund, did not violate federal law, but the federal government violated his rights. Based on the statutory language of the CFAA, Leomund could not have violated the statute as it does not criminalize acts for which one had authorization, and did not exceed such authorization, to commit. Additionally, the police and FBI investigators wrongfully exceeded the limits of the Fourth Amendment by extensively searching Leomund without a warrant.

The CFAA's liability-inducing phrase "without authorization" does not include impermissible use as a manner of criminal misconduct. In fact, the statute should be given a much narrower interpretation, as the plain language reading would suggest. Congress did not intend for this anti-hacking statute to introduce broad liability, nor was it meant to be a misappropriation statute. While Leomund's actions may have been contrary to his employer's Use Policies, such minor workplace violations should not constitute federal crimes. As the CFAA's text should be interpreted narrowly, Leomund cannot be guilty of violating the statute under the "without authorization" prong of liability.

Similarly, Leomund cannot be found to have violated the "exceeding authorized access" prong of CFAA liability, as criminal liability here cannot be based on agency principles. Only one circuit court has taken to applying agency principles in this context, and no other circuit court has followed. Should this Court decide with the minority, it would soon be faced with non-delegation issues and an unworkable statute. Allowing agency principles to govern liability essentially allows private actors, such as employers, and prosecutors to define the scope of the statute's liability – a job clearly tasked to Congress. Therefore, agency principles cannot apply and thus Leomund cannot be found guilty of violating the CFAA under this prong either.

Additionally, all evidence collected against Leomund should be suppressed as the Government violated his Fourth Amendment right against an unreasonable search without a warrant. Leomund was unknowingly and extensively searched over a period of two and a half weeks. Multiple methods of surveillance and multiple technological devices were put to use to monitor Leomund's every movement and activity over those weeks of surveillance. As Leomund subjectively held a reasonable expectation of privacy during this time, the Supreme Court must

hold that such detailed and comprehensive information gathering constitutes an unconstitutional search without a warrant.

This is certainly a case of the Government trying to stretch the boundaries of both its interpretative powers and searching capabilities. However, finding in favor of the Government here has broad implications for employees across the country as well as severe consequences for the population generally with regards to an individual's right to privacy.

ARGUMENT

The Court should reverse the appellate court's decision and find in favor of petitioner, Gerrard Leomund, by dismissing the CFAA claims and affirming the motion to suppress evidence, because the CFAA is a narrow statute which does not cover Leomund's action and because the police and FBI unreasonably searched Leomund without a warrant.

I. STANDARD OF REVIEW

This court reviews all lower courts' grants of a motion to dismiss *de novo*. *See Gilbert v. Residential Funding LLC.*, 678 F.3d 271, 275 (4th Cir. 2012). The burden is on the plaintiff to set forth a plausible claim for relief in order to survive a motion to dismiss, which requires "more than the mere possibility of misconduct." *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). The Court need not give deference to legal conclusions from lower courts. *Iqbal*, 556 U.S. at 678.

On questions of statutory interpretation, the Court also applies *de novo* review. *See United States v. Rahim*, 431 F.3d 753, 756 (11th Cir. 2005). When interpreting a statute which has both civil and criminal provisions, such as the CFAA, the task "merits special attention

because [the court's] interpretation applies uniformly in both contexts." *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004). When interpreting criminal statutes, the Court must apply the canon of strict construction, also known as the rule of lenity. *United States v. Lanier*, 520 U.S. 259, 266 (1997). Of course, in making their interpretations courts should avoid a result that leads to patently absurd consequences. *United States v. Brown*, 333 U.S. 18, 27 (1948). Additionally, in the interest of providing officers rules and guidelines for how to conduct legal searches, *de novo* review is preferred for Fourth Amendment search and seizure questions. *Ornelas v. United States*, 517 U.S. 690, 697-98 (1996).

II. THE PLAIN LANGUAGE, CONGRESSIONAL INTENT, AND PRACTICAL IMPLICATIONS OF THE COMPUTER FRAUD AND ABUSE ACT NECESSITATE A READING OF "WITHOUT AUTHORIZATION" IN THE CFAA TO ONLY PROTECT AGAINST UNAUTHORIZED ACCESS AND NOT UNAUTHORIZED USE.

Broadening the term "without authorization" in the CFAA to encompass unauthorized use is inconsistent with the plain language of the statute and clear congressional intent, and leads to demonstrably unworkable results. The question of whether or not the CFAA contemplates criminalizing unauthorized use in addition to unauthorized access is necessarily a question of statutory interpretation, which hinges on the text, purpose, and practical implications of the statute. Although the plain language and legislative history make clear that the statute does not encompass the broader conduct of use, the court may also consider the absurd results that may occur should CFAA liability attach to violations of company use policies. Further, if this Court were to find ambiguity in the statute's language, the rule of lenity would mandate that any ambiguity be resolved in favor of Leomund.

A. The Plain Language Interpretation of the Statute Does Not Include Unauthorized Use.

First and foremost, the plain language of the statute mandates a dismissal of respondent's claims. In relevant part, the CFAA reads, "[w]hoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--information from any department or agency of the United States." 18 U.S.C. § 1030(a)(2)(B).

The statute speaks explicitly in terms of access and *not* use. When interpreting statutes, courts look to the "full text, language as well as punctuation, structure, and subject matter" to determine a statute's meaning. *U.S. Nat'l Bank of Or. v. Indep. Ins. Agents of Am., Inc.*, 508 U.S. 439, 455 (1993). The Ninth Circuit determines a statute's plain meaning by "examining the statute's language as well as its object and policy." *United States v. Flores-Garcia*, 198 F.3d 1119, 1121 (9th Cir. 2000). The Fourth Circuit directs courts to give the statutory terms their ordinary meaning, absent a clear indication from Congress that a different meaning was meant. *Stephens ex rel. R.E. v. Astrue*, 565 F.3d 131, 137 (4th Cir. 2009).

Under the plain language reading of the CFAA, the relevant portion only purports to prohibit unauthorized *access*. Nowhere in the statute is there language which would sweep so broadly as to capture impermissible use. "Authorization" as written in the CFAA is meant to be interpreted in "common usage, without any technical or ambiguous meaning." *United States v. Morris*, 928 F.2d 504, 511 (2d Cir. 1991). The plain language reading of the CFAA supports a narrow reading of the stature and the specific provision at issue.

In common understanding, access is defined as "[t]o obtain, acquire," or "[t]o gain admission to." *Oxford English Dictionary* (3d. ed. 2011; online version 2012). The dictionary defines authorization as "permission or power granted by an authority." *Random House*

Unabridged Dictionary, 139 (2001). The Ninth Circuit's plain language reading of "without authorization" in the CFAA translates to without permission. *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009). Similarly, the Fourth Circuit has stated that an employee "accesses a computer 'without authorization' when he gains admission to a computer without approval." *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012). Here, the plain meaning of the statute is clear as it applies to Leomund. Congress spoke in terms of access and not use, and therefore the CFAA claim should be dismissed. As interpreted by the courts, dictionaries, and as intended by Congress, authorization was meant to capture access and not use.

B. The Legislative History of the CFAA Evinces a Clear Congressional Intent to Limit Liability Under the CFAA to Circumstances Involving Unauthorized Access and Not Unauthorized Use.

To buttress the plain language interpretation of the CFAA that authorized access does not encompass "use" inquiries, the legislative history forecloses the Government's suggested reading that the CFAA criminalizes unauthorized use. It is worth repeating that the relevant portion of the statute reads, "[w]hoever intentionally *accesses* a computer without *authorization*…" 18 U.S.C. § 1030(a)(2)(B)(2012)(emphasis added).

The CFAA was originally passed in 1986, but has been amended several times. One of the earliest amendments was passed with the intention of clarifying "one of the murkier grounds of liability." S. Rep. No. 99-432, at 21 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2494. This amendment demonstrates a clear intent to remove any "murkiness" that improper use or misappropriation theories could lead to CFAA liability. *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 966 (D. Ariz. 2008). Courts consistently recognize that the legislative history reveals the purpose of the CFAA is to target outside computer hackers. *A.V. ex rel. Vanderhye v.*

iParadigms, LLC, 562 F.3d 630, 645 (4th Cir. 2009) (recognizing the CFAA is a statute "generally intended to deter computer hackers"); *US Bioservices Corp. v. Lugo*, 595 F. Supp. 2d 1189, 1193 (D. Kan. 2009) ("The CFAA was intended as a criminal statute focused on 'hackers' who trespass into computers, and the statute deals with unauthorized access in committing a computer fraud rather than the mere use of a computer."); *Shamrock Foods Co.*, 535 F. Supp. 2d at 965 (Relying on Senate reports, the court recognized the purpose of the CFAA was to deter computer hackers and to address unauthorized access "rather than the mere use of a computer").

When contemplating criminal liability, the statute asks whether the initial access of a computer was authorized and not whether the use of information gained through access was authorized. Broadening the clear terms "intentionally accesses" and "without authorization" to capture unauthorized uses would transform the statute into a creature not envisioned by Congress. The purpose of the CFAA was to target hackers, not disloyal employees. *Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479, 495 (D. Md. 2005). The term "without authorization" refers clearly to "a situation where an outsider, or someone without authorization, accesses a computer." *In re AOL, Inc. Version 5.0 Software Litig.*, 168 F. Supp. 2d 1359, 1370 (S.D. Fla. 2001).

As was explained by the district court below, legislative history also indicates that "the conduct prohibited is analogous to that of 'breaking and entering' rather than using a computer (similar to the use of a gun) in committing the offense." H.R. Rep. No. 98-894, at 20 (1984). The court in *Dresser-Rand* considers an analogy to burglary which illustrates the necessary distinction between access and use: "If a person is invited into someone's home and steals jewelry while inside, the person has committed a crime--but not burglary--because he has not broken into the home. The fact that the person committed a crime while inside the home does not

change the fact that he was given permission to enter." *Dresser-Rand Co. v. Jones*, 957 F. Supp. 2d 610, 614 (E.D. Pa. 2013). To interpret "access without authorization" in a way that folds in "unauthorized use" would directly contravene the explicit intent of Congress and other courts' interpretations of Congress' purpose while consequently rendering the term meaningless.

As Congress both intended and drafted the statute, Leomund's activity simply does not fall within the scope of criminal liability under the CFAA. Because at all relevant times, Leomund had the authority to access the CDC-Secure database it cannot be argued that he violated the "without authorization" prong of the CFAA. Leomund was an employee of the CDC and not the sort of dark room hacker that Congress was intending to capture. When drafting the CFAA Congress certainly did not have in mind that it would be criminalizing activity similar to Leomund's. The common understanding of the term and the intended Congressional meaning foreclose the possibility of liability here.

C. Reading the CFAA in a Manner That Encapsulates Unauthorized Use Would Impermissibly Transform the CFAA From a Hacking Statute Into a Misappropriation Statute.

Courts in a plurality of circuits have held that reading "unauthorized use" into the CFAA would inappropriately render it a misappropriation statute. *See Brekka*, 581 F.3d at 1127. The Ninth Circuit's interpretation is that "if an employee accesses information from a computer within his permissible parameters, regardless of his subsequent disloyal treatment of that information, he is neither accessing the computer without authorization nor exceeding his authorized access and, therefore, does not violate" the CFAA. *Consulting Prof'l Res., Inc. v. Concise Tech. LLC*, Civil Action No. 09-1201, 2010 WL 1337723, at *5 (W.D. Pa. March 9, 2010) (referring to *Brekka*, 581 F.3d at 1135.). This interpretation is consistent with both the plain language of the statute and the intent of Congress.

While the distinction seems narrow, courts are cognizant that access and use are crucially distinguishable and should not be confused. *Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007); *Bell Aero. Servs. v. U.S. Aero. Servs.*, 690 F. Supp. 2d 1267, 1272 (M.D. Ala. 2010). The scope of the CFAA does not encompass "[w]hatever happens to the data subsequent to being taken from the computers." *Dresser-Rand Co.*, 957 F. Supp. 2d at 615. Courts cannot hinge liability under the "authorized access" prong of the CFAA based upon conduct that occurs after an employee's authorized access. *Brett Senior & Assoc., P.C. v. Fitzgerald*, Civil Action No. 06-1412, 2007 WL 2043377 at *3 (E.D. Pa. July 13, 2007). While courts may rightfully be concerned about the activity that may result after authorized access, it is not their role to foray into the field of redrafting the statute to capture activity that they consider wrongful. In fact, the CFAA does "not prohibit the unauthorized disclosure or use of information, but rather unauthorized access. Nor do their terms proscribe authorized access for unauthorized or illegitimate purposes." *Werner-Mastuda*, 390 F. Supp. 2d at 499.

Courts have found that subsequent misuse of data accessed with authorized permission was irrelevant for the purpose of finding CFAA liability. *Bell Aero. Servs. v. U.S. Aero Servs.*, 690 F. Supp. 2d at 1272. Additionally, when employers grant unrestricted employee access to computers, a finding of misappropriating data does not constitute a CFAA violation. *Lasco Foods, Inc. v. Hall & Shaw Sales, Mktg., and Consulting LLC*, 600 F. Supp. 2d 1045, 1053 (E.D. Mo. 2009). *But see United States v. John*, 597 F.3d 263, 271 (5th Cir. 2010) (finding "authorization" to limit the use of information only "when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a crime"). The so called "intended-use analysis" that the

Fifth Circuit used in *John* is not applicable here since Leomund still had authorized access to the entire database even in his re-assigned role.

Merely because Leomund may have improperly used the information he gathered from the CDC-Secure system does not necessitate that his initial access was also improper. The Government cannot turn back the clock and make Leomund's initial access criminal simply because he used the information gained for improper means. When Leomund obtained the information, he was authorized to do so based on the evidence that his username and password allowed him to enter the system. Once inside the system, Leomund had authorized access to all information it contained. If the CDC is so concerned with the security of its information, it should have organized and secured the database in a way that allows employees to only gain access to information with which they are directly involved. The burden should not be on an employee such as Leomund to navigate the database like a minefield while hoping to not accidentally open a document that was not meant for his eyes.

D. CFAA Liability Should Not Hinge on an Employee's Adherence to Employer Use Policies as Such Conduct Does Not Necessarily Warrant Criminal Prosecution and Policies Frequently Change.

There cannot be liability under the CFAA based solely on an employee's failure to comply with an employer's Terms of Use as that could produce absurd results for employees. *WEC Carolina Energy Sol., LLC*, 687 F.3d at 207. In *WEC Carolina Energy Solutions*, the Fourth Circuit dismissed the plaintiff's suit for failure to state a claim, stating that the CFAA concerns impermissible access and that liability cannot be based solely on a violation of company use policy. *Id.* The *WEC Carolina Energy Solutions* court explicitly recognized that holding employees criminally liable for disregarding an employer use policy would contravene Congress' intent. *Id.* The court noted that allowing employer use policies to dictate CFAA

liability "would impute liability to an employee who with commendable intentions disregards his employer's policy against downloading information to a personal computer so that he can work at home," as he would have "obtained information 'in a manner' that was not authorized." *Id.* at 206.

The Ninth Circuit explored the consequences of imputing criminal liability based on a violation of a computer use policy in *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012). "[U]se policies can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved." *Nosal*, 676 F.3d at 860. Given the frequency and ease with which employers change use policies, courts should be cautious of imposing criminal liability on an employee whose conduct, which was permissible on Monday, became criminal on Tuesday solely because their employer updated the Terms of Use for their computers. Terms of Use restrictions are often lengthy and essentially contracts of adhesion. Allowing a violation of employer use policies to give rise to CFAA liability gives tremendous power to the CDC and other employers.

E. The Rule of Lenity Mandates a Narrow Interpretation of "Unauthorized Access," which Excludes Criminalizing Unauthorized Use, so as to Provide Fair Warning to Potential Actors.

While the plain language reading of the CFAA and its legislative history unambiguously support a narrower interpretation of "without authorization," should this Court disagree, the rule of lenity must apply to ensure "fair warning by so resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered." *United States v. Lanier*, 520 U.S. at 266. The rule of lenity instructs "penal laws...to be constructed strictly." *United States v. Wiltberger*, 18 U.S. 75, 95 (1820). "[D]ue process bars courts from applying a novel construction of a criminal statute to

conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope." *Lanier*, 520 U.S. at 266.

The Fourth Circuit applied this rule to the CFAA when it rejected a broad interpretation of "without authorization," noting that Congress is the proper entity to impose a harsher reading of a criminal statute, not the court. *WEC Carolina Energy Solutions, LLC*, 687 F. 3d at 206. The scope of CFAA liability should be narrowly construed to protect individuals from being caught off guard with criminal liability, as opposed to the broad interpretation supported by the Government, which could encompass innocuous and well-intentioned conduct. The court should be hesitant of interpreting "unauthorized access" broadly as the *Nosal* court, among others, has demonstrated, a broad reading can easily criminalize seemingly innocent employee behavior. If this court determines that the statutory language is ambiguous, the rule of lenity should be applied and the language narrowly read.

Holding Leomund liable under the CFAA for his misuse of information is inappropriate, and, given the facts of this case, is tantamount to forcing a square peg in a round hole. It cannot be argued that Leomund was on notice that his activity could be criminal under the CFAA. Collapsing unauthorized use into "without authorization" steers the law into unchartered territory of which employees cannot reasonably be held to be aware. Relatedly, the government cannot paint this as a scenario where the court is faced with either convicting Leomund under this broad reading or allowing similar actors to walk free without punishment. The government is not without redress, as Leomund may potentially be held liable under a number of other legal claims, including trespass, misappropriation of trade secrets, theft, and breach of contract. However, expanding the scope of an anti-hacking statute to capture the conduct at issue here is inappropriate and unwise considering the plain language of the statute, congressional intent,

widely-held interpretations in other jurisdictions, policy considerations, and rules of statutory construction. The court should hold that "without authorization" does not encompass unauthorized use within CFAA liability.

III. AGENCY PRINCIPLES ARE NOT THE PROPER TOOL TO GIVE COLOR TO THE PHRASE "EXCEEDS AUTHORIZED ACCESS".

The phrase "exceeds authorized access" is defined by the statute as to "access a computer with 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). Put another way, a person who "exceeds authorized access" is one who "accesses information on the computer that the person is not entitled to access." *Brekka*, 581 F.3d at 1133. Beyond the explicit text of the statute, the Court can look to how other courts have interpreted the term, and consider other guiding principles relevant to interpretation.

A. *Citrin* was Wrongly Decided and Should Not Be Followed by the Court.

The Seventh Circuit's opinion in *International Airport Centers, LLC v. Citrin* is perhaps the leading, and only, authority for the theory that agency and fiduciary duty principles should govern the phrase "exceeds authorized access." 440 F.3d 418 (7th Cir. 2006). While the Seventh Circuit acknowledges that "[t]he difference between 'without authorization' and 'exceeding authorized access' is paper thin," the difference is important and the two should not be conflated to mean the same thing. *Citrin*, 440 F.3d at 420. Although the Seventh Circuit is correct that the difference between the terms is elusive, the court incorrectly settles on agency principles to give color to the distinction.

In *Citrin*, an employee was issued a laptop from his employer. Upon deciding to quit, the employee returned his laptop to the employer, but not before loading a secure-erasure program to

the laptop which deleted all data and prevented its recovery. *Id.* at 419. The court determined that "his authorization to access the laptop terminated when, having already engaged in misconduct and decided to quit IAC in violation of his employment contract, he resolved to destroy files that incriminated himself...in violation of the duty of loyalty that agency law imposes on an employee." *Id.* at 420. The Seventh Circuit's agency approach would require courts to delve into the intentions and motivation of an employee when he or she is accessing a computer. *Id.* at 420-21. That court held that the employee's "breach of his duty of loyalty terminated his agency relationship… and with it his authority to access the laptop, because the only basis of this authority had been that relationship." *Id.*

In implementing agency principles, the Seventh Circuit is essentially criminalizing conduct that was initially permissible. For example, under the *Citrin* approach, an individual could log in to their computer with authorized access, but then engage in conduct contrary to the interest of his employer, however slight, and consequently the valid authorization the employee held would seemingly evaporate. This conflates not only access and use, but also erases the important distinction between "without authorization" and "exceeds authorized access" portions of the CFAA.

Under the agency theory, it is easy to hypothesize absurd results as to when criminal liability under the CFAA could be imposed. *Nosal*, 676 F.3d at 860. The Ninth Circuit considered several of these absurd results that come from all too common everyday scenarios when it expressly rejected the *Citrin* approach in deciding *Nosal*. For example,

> [e]mployees who call family members from their work phones will become criminals if they send an email instead. Employees can sneak in the sports section of the *New York Times* to read at work, but they'd better not visit ESPN.com. And sudoko enthusiasts should stick to the printed puzzle, because visiting www.dailysudoko.com from their work computers might give them more than enough time to hone their sudoko skills behind bars.

Id.

While the result of these hypothetical situations may seem far-fetched, the situations are all too common in the daily work environment. Yet under the *Citrin* agency approach, anytime an employee engages in conduct contrary to the interest of the employer he loses authority to access that computer and can potentially face criminal liability under the CFAA.

B. No Other Circuits Have Adopted *Citrin*'s Agency Law Theory

The fact that no other circuit court has adopted the *Citrin* approach is telling and should prove as a caution to this Court before deciding to follow the Seventh Circuit down this lonely road of applying agency law principles to the CFAA. Among the greatest concerns against adopting an agency theory is the fact that such an interpretation would "collapse the independent requirements of the statute into a single inquiry." *Dresser-Rand*, 957 F. Supp. 2d at 619 (citing *Brett Senior & Assoc., P.C. v. Fitzgerald*, No. 06-1412, 2007 WL 2043377, at *4 (E.D. Pa. July 13, 2007)). Therefore, not only would this be contrary to legislative intent, the use of agency principles here would be incompatible with the CFAA and prove the statutory framework to be incoherent.

An agency theory would fail to give meaning and effect to the distinct sections of the statute and thus a number of courts have declined to adopt a fiduciary duty of loyalty approach to the CFAA. *See Nosal*, 676 F.3d at 862; *WEC Carolina Energy Solutions, LLC*, 687 F.3d at 206; *Bridal Expo, Inc. v. Van Florestein*, Civil Action No. 4:08-CV-03777, 2009 WL 255862, at *10 (S.D. Tex. Feb. 3, 2009); *Brett Senior*, 2007 WL 2043377, at *18. In declining to rely on agency principles to allow an individual's intent to govern CFAA liability, the court in *Brett Senior* astutely noted that "[i]t is unlikely that Congress, given its concern 'about the appropriate scope

of Federal jurisdiction' in the area of computer crime, intended essentially to criminalize state-law breaches of contract." *Brett Senior*, 2007 WL 2043377, at *13-14.

Courts have recognized that since it was not Congress' intent to have CFAA liability turn on an individual's intentions, the statute could not be interpreted as such. *See Brekka*, 581 F.3d at 1135; *Lewis-Burke Assoc. LLC v. Widder*, 725 F. Supp. 2d 187, 194 (D.D.C. 2010). The D.C. Circuit surmised that "Congress could not have intended a person's criminal and civil liability to be so fluid," and therefore declined to find liability based on whether an individual's interests were adverse to his employer's. *Widder*, 725 F. Supp. 2d at 194. The Ninth Circuit reasoned that such an interpretation would leave defendants with "no reason to know that making personal use of the company computer in breach of a state law fiduciary duty to an employer would constitute a criminal violation of the CFAA." *Brekka*, 581 F.3d at 1135.

C. Applying Agency Principles to the CFAA Gives Rise to Significant Private Non-Delegation Concerns

A broad interpretation of the CFAA which employs agency principles essentially grants prosecutors and private parties the authority to decide which conduct rises to the level of warranting criminal punishment, and such a delegation of authority is impermissible. *United States v. Kozminski*, 487 U.S. 931 (1988); *Carter v. Carter Coal Co.*, 298 U.S. 238 (1936). This sort of authority is legislative in nature and should be left to Congress. If Congress intended agency law to govern the CFAA, they would have been explicit in the statute. The consequence of this agency approach is that private entities, through their drafting of use and access restrictions, can delineate what is permissible for an employee, and consequently what is criminal. In addition to the illegal transfer of law-making power, such an interpretation undermines the legislative intent of Congress. *Dresser-Rand*, 957 F. Supp. 2d at 619. As at least

one court has noted, "there is no mention of agency or loyalty in the CFAA, statute that was designed to punish computer hackers." *Id.*

Applying agency principles in Leomund's situation highlights the problems discussed above. If the Court were to undertake the agency approach, it would require a fact intensive effort into the subjective intent and motive of Leomund. If he had acceptable intentions when logging into the system, these do not evaporate simply because his later use deviates from the best interest of his employer. Application of agency principles can lead to unworkable and arbitrary distinctions while criminalizing innocent behavior. If Leomund, while assigned to Phyresis research on behalf of the CDC, decided to look into cancer statistics after hearing of a personal friend's cancer diagnosis, he would arguably have violated the CFAA under an agency approach. This result is just one of countless troublesome outcomes that can and will arise if this Court deviates from the majority approach of interpreting "exceeds authorized access."

IV. POTENTIALLY REASONABLE SEARCHES UNDER THE FOURTH AMENDMENT MAY BE RENDERED UNREASONABLE WHEN CONSIDERED IN THE AGGREGATE.

The Fourth Amendment has long provided citizens protection from unreasonable intrusions by the government, specifically providing that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, should not be violated." U.S. Const. amend. IV. A search can occur whenever there has been a physical trespass by the government. *United States. v. Jones*, 132 S. Ct. 945, 949 (2012). Additionally, courts may consider whether the individual exhibited an actual expectation of privacy and whether that expectation was reasonable. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

A search without a warrant is per se unreasonable, with a few narrow exceptions. *Id.* at 357. As most of the narrow exceptions are inapplicable to this case, this brief will only discuss the plain view doctrine as it applies here. The plain view doctrine holds that police may seize evidence that is in the officer's plain view, as there is a diminished expectation of privacy, so long as the officer does not violate the Fourth Amendment in getting to the position where the evidence could be seen. *Id.* at 361.

However, even this exception may run afoul of a reasonable expectation of privacy if used to justify multiple searches which result in substantial and detailed data regarding one's life. Additionally, if the effects of such searches are not evaluated in the aggregate, individuals could be subjected to large-scale police monitoring without any judicial review. Lastly, one's home and surroundings are given the utmost importance in regards to Fourth Amendment privacy concerns.

A. Individuals have a Reasonable Expectation that the Government Will Not Be Able to Paint an Intimate Picture of Their Lives Through the Collection of Substantial Amounts of Data Without a Warrant.

While *United States v. Jones* was resolved on physical trespass grounds, members of the Court advocated evaluating searches based on the totality of evidence collected and the nature and detail of information discovered during surveillance. 132 S. Ct. 945 (2012). *Jones* involved an individual who was monitored for 28 days when the government installed a GPS on the undercarriage of his car without a valid warrant. *Id.* at 948.

In an oft-cited concurrence, Justice Sotomayor focused on the cumulative intrusion of even short-term monitoring when it produces a comprehensive and detailed record of an individual's public, yet intimate, actions. *Id.* at 955. Justice Sotomayor cites a New York case to describe the sorts of intimate details gathered through such monitoring, such as "trips to the

psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *Id.* (citing *People v. Weaver*, 909 N.E.2d 1195, 1199-1200 (N.Y. 2009)). Sotomayor did not find efficiency to be a sufficient or dispositive argument in favor of using such comprehensive police tactics, and instead, focused the inquiry on whether individuals reasonably expect to be monitored in a manner that allows the government to discover "their political and religious beliefs, sexual habits, and so on." *Id.* at 956.

In a concurrence joined by Justices Ginsburg, Breyer, and Kagan, Justice Alito analyzed the facts in *Jones* under the expectation of privacy test articulated in *Katz*. *Id.* at 958. Justice Alito's concurrence emphasized the length of time monitored in relation to one's expectations of privacy, and, without drawing a bright line, found that the line between permissible surveillance and an unconstitutional search "was surely crossed before the 4-week mark." *Id.* at 964. His opinion also noted the ability of police officers to seek a warrant for these extensive searches. *Id.*

While the Supreme Court declined to decide *Jones* on expectation of privacy grounds, the D.C. Circuit, in deciding the same case, held that prolonged surveillance of the whole of a person's movements and activities constitutes a search. *United States v. Maynard*, 615 F.3d 544, 561 (D.C. Cir. 2010), *aff'd on other grounds*, *United States v. Jones*, 132 S. Ct. 945 (2012). Noting the idea that "the whole may be more revealing than the parts," the D.C. Circuit found the GPS tracking device's extensive travel records over time to provide the government with too detailed of information about the defendant's life to be permissible. *Id.* at 562-63. The D.C. Circuit concluded that while each individual action by the defendant may have occurred in public view, the extensive compilation of movements and actions taken were not exposed to the public, such that the defendant would not have expect a single person to observe all of it. *Id.* at 560.

In recent years, courts have shown unease with the government's use of technology not available to the general public, such as cell site location information ("CLSI"), to monitor a target. *United States v. Graham*, 796 F.3d 332 (4th Cir. 2015), *reh'g granted*, No. 12-4659, 2015 WL 6531272 (Oct. 28, 2015). In *Graham*, the Fourth Circuit held that because an inspection of CLSI allows for the "government to trace the movements of the cell phones and its user… and thereby discover the private activities and personal habits of the user," it constituted a search requiring a warrant. *Id.* at 344-45. Analogizing to GPS tracking cases, the court emphasized the "individual's privacy interests in comprehensive accounts of her movements… particularly when such information is available only through technological means not in use by the general public." *Id.* at 345. Additionally, the court held that such privacy interests are unconstitutionally infringed upon by the government when an individual is monitored over a time period as short as 14 days. *Id.* at 350.

Circuit courts that have rejected the notion that individuals have a reasonable expectation of privacy regarding cell phone data rely on the fact that this data is voluntarily relayed to cellular service providers, rather than compelled into collection by the government. *In re U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013); *United States. v. Davis*, 785 F.3d 498 (11th Cir. 2015). In *Historical Cell Site Data*, the court also noted diminished infringement on privacy interests where the government sought cell phone data to determine where a suspect had gone in the past few weeks. 724 F.3d at 601. Similarly, in *Davis*, the government sought weeks of historical cell tower location data, as opposed to any real-time data. 785 F.3d at 501. However, the Fourth Circuit disagrees with those characterizations of the privacy expectation as such data is collected by the service provider "without the user's active participation," and that even if the user knows the cell provider collects information, he does not necessarily know of the

risk of disclosure to law enforcement. *Graham*, 796 F.3d at 355. Similarly, courts have struggled with where to draw the line on the monitoring of real-time cell phone data. *See United States v. Skinner*, 690 F.3d 772, 777 (6th Cir. 2012) (holding no expectation of privacy where defendant voluntarily used pay-as-you-go cell phone, which emitted a location signal tracked by police); *United States v. White*, 62 F. Supp. 3d 614 (E.D. Mich. 2014) (finding a violation of privacy where defendant's borrowed cellphone was tracked continuously for weeks).

Here, the FBI and local police's comprehensive surveillance of Leomund violated his reasonable expectation of privacy as it revealed intimate details of his life. Like the defendant in *Weaver*, cited by Justice Sotomayor in *Jones*, the government tracked Leomund on trips of an indisputable private nature, such as to the urologist's office, gentleman's clubs, and the psychiatrist's office. J.A. at 15. In *Jones*, Justice Alito's concurrence found the government to have infringed on the privacy expectation based on less than four weeks of GPS tracking. Here, while the government's surveillance took place over a total of 17 days, the monitoring was arguably more comprehensive than just GPS data, as the information collected covered not just where Leomund went, but who visited his home, when he arrived and left his home, and what was occurring in his own backyard.

Similarly, while Leomund's actions each took place in the public eye, he would not have expected for each movement to have been viewed by the same person, as was done by the government. Leomund was tracked with a similar level of intrusiveness as the defendant in *Maynard*. It was not Leomund's expectation that any member of the public would have followed all of his actions that extensively, and therefore he held a reasonable expectation of privacy regarding the detailed information people gathered about his daily life.

While the investigators did not scour Leomund's cell phone data, they relied on similar large-scale data collection in the form of the license-plate scanner and constant video surveillance of his home. Like the defendant in *Graham*, Leomund was unknowingly subjected to over two weeks of data collection. However, unlike the defendants in *U.S. Historical Cell Site Data* and *Davis*, Leomund never consented to sharing any of this information with third parties. Nowhere in the record does it indicate that Leomund's travels required him to relay information to third parties, not even in the form on taxi cab fares or paying tolls on public roads. Nor did Leomund ever convey information about his comings and goings from his home or activities in his backyard to others. Cumulative information on Leomund's location and activities over time should be afforded a reasonable expectation of privacy, as was recognized by multiple Justices in *Jones*, as well as the Fourth Circuit in *Graham*.

B. Society Recognizes as Legitimate the Privacy Expectations that Individuals Will Not Be Subject to Large-Scale Police Monitoring Without Judicial Review.

Society has generally understood warrantless police surveillance to be limited by a number of factors, despite the fact that technology is quickly negating these limitations. In Justice Alito's concurring opinion in *Jones*, he describes society's expectation as one in which "law enforcement agents and others would not – and indeed, in the main, simply could not – secretly monitor and catalogue every single movement of an individual's care for a very long time." 132 S. Ct. at 946. Similarly, Justice Sotomayor describes in her concurrence "the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility'," which are absent when advanced technologies are used in place of conventional surveillance techniques. *Id*. at 956 (citing *Illinois v. Lidster*, 540 U.S. 419, 422 (2004)). In *Maynard*, the D.C. Circuit stated that when "monitoring reveals an intimate picture of

the subject's life that he expects no one to have—short perhaps his spouse," the government has trampled on the reasonable expectation of privacy. 615 F.3d at 563.

Concerns over the workability of analyzing whether aggregate data collection constitutes a search should not cast doubts on society's recognition of this as a legitimate privacy interest. Like every other Fourth Amendment search inquiry, cases involving multiple monitoring techniques by the government should be "decided on the facts of each case, not by extravagant generalizations." *Dow Chemical Co. v. United States*, 476 U.S. 227, 238 n.5 (1986). Courts must set forth the constraints on the government to harness the "power of technology to shrink the realm of guaranteed privacy." *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

Just as with other Fourth Amendment inquiries, courts should engage in a balancing test, weighing "the nature and the quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion." *United States v. Place*, 462 U.S. 626, 703 (1983). Under such an inquiry, the more pressing the government's reasons for longer surveillance, such as in cases of domestic terrorism, the less justification needed. *White*, 62 F. Supp. 3d at 624. However, when the government's reasons underlying the need for prolonged surveillance are not critical, then more justification will be required to sustain such monitoring. *Id.* Similarly, the "nature and quality" of the surveillance can tip the balance in favor of protection of the individual, and requiring "the state to demonstrate probable cause as a justification for the intrusion." *Id.* Nature and quality may go to the length of time the individual was monitored by the government, or to the extent and level of detail at which information was collected. *Id.*

Society recognizes as legitimate Leomund's privacy interest in not being so thoroughly tracked and intimately monitored without a warrant. This type of interest is exactly what Justice

Alito described in his opinion in *Jones*. Society expects that citizens will not be comprehensively tracked in the manner in which Leomund was here – almost, in total, his every move. While in the past society expected that police time and resources would properly cabin these kinds of searches, cost and convenience of observation tactics cannot supplant the calculus for determining when judicial oversight is needed. As was described in *Maynard*, society does not expect the police to gather as much information about an individual's daily life as is known only by him and his spouse.

While it is difficult to draw definitive lines of what society recognizes as legitimate expectations of privacy, the Court need only decide the case before it. Cases involving the legitimacy of multiple searches when analyzed in the aggregate must be approached on a case-by-case basis; however, comprehensive surveillance should be evaluated in its entirety to determine if it constitutes a reasonable search. To rule otherwise is to allow the police to do what they did to Leomund to others, which was 17 days of invasive surveillance that resulted in the accumulation of personal and intimate data on an individual, yet claim that they never "searched" him. Analyzing only each individual hit on a license plate scanner, or each image of a continuously recording pole camera, neglects the great amount of data the police are collecting on individuals. Without such a comprehensive analysis available to the lower courts, individuals must be prepared to be watched by their government at all times after leaving the four walls of their homes.

C. The Sanctity of the Home and Surrounding Area is of Paramount Importance under the Fourth Amendment Protections.

The areas surrounding one's home, also known as curtilage, carry the same kind of protection from government intrusion as the home itself. *United States v. Dunn*, 480 U.S. 294,

300 (1987). The Court in *Dunn* set forth four factors to consider when determining whether a space is curtilage, and thus has heightened protection: "the proximity of the area claimed to be curtilage to the home, whether the area is included within an enclosure surrounding the home, the nature of the uses to which the area is put, and the steps taken by the resident to protect the area from observation by people passing by." *Id.* at 301. Courts have already extended the definition of curtilage to cover yards near one's home. *See United States v. Anderson-Bagshaw*, 509 F. App'x 396, 404 (6th Cir. 2014) (designating as curtilage back yard area containing furniture, such as a picnic table and gazebo, indicating use for domestic purposes); *United States v. Vargas*, No. CR-13-6025-EFS, (E.D. Wash. Dec. 15, 2014) (applying curtilage designation to front yard used for socializing in a rural area).

The plain view exception as applied to curtilage does not allow the government to monitor areas that would not otherwise be visible by the naked eye nor is it permitted to gather intimate details about one's life under the guise of this exception. *California v. Ciraolo*, 476 U.S. 207, 213 (1986); *Dow Chem. Co. v. United States*, 476 U.S. at 238. In *Ciraolo*, police used aerial observation to view marijuana plants in a suspect's backyard where the plants were visible to the naked eye from the plane. 476 U.S. at 209. While holding such observation permissible, this Court cabined this surveillance to "observations from a public vantage point where [an officer] has a right to be and which renders the activities *clearly* visible." *Id.* at 213 (emphasis added). In *Dow Chem. Co.*, this Court permitted into evidence photographs, later to be enhanced, taken by the Government of an area surrounding an industrial plant. 476 U.S. at 229-30. However, the Court also noted the Government's concession "that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public… might be constitutionally proscribed absent a warrant." *Id.* at 238. Additionally, the Court emphasized that

the commercial property at issue was not to receive the same heightened protection as curtilage adjacent to a home in regards to aerial surveillance. *Id.* at 239.

While areas considered curtilage are subject to the plain view exception, police cannot use intrusive forms of technology to monitor areas where there is an expectation of privacy. *Kyllo*, 533 U.S. at 40. In *Kyllo*, police used thermal imagers to detect high-intensity lamps used to grow marijuana within the house. *Id.* at 29-30. This Court has held that the police's use of "sense-enhancing technology" to obtain information "that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area'" constituted an unconstitutional search as the thermal imagers were not a technology in general public use. *Id.* at 34 (citing *Silverman v. United States*, 365 U.S. 505, 512 (1961)). Evidence gathered through technology not in common use, which makes visible that which was not visible without physical intrusion, is the product of an unreasonable search.

Similarly, police officers cannot use electronic surveillance devices to obtain information from inside the home when such information could not have been observed "from outside the curtilage of the house." *United States v. Karo*, 468 U.S. 705, 715 (1984). In *Karo*, police placed a beeper inside of a can which the target then unknowingly took inside his home. *Id.* at 708. The Court held that "monitoring a location not open to visual surveillance" constituted an unreasonable search as the surveillance device revealed "a critical fact about the interior of the premises that the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant." *Id.* at 714-15. When the police use technology to invade a space in which an individual has a reasonable expectation of privacy, such as their home and curtilage, then it is an unreasonable search and all evidence gathered must be suppressed, save for a few narrow exceptions not at issue here. *But see United States v. Knotts*, 460 U.S. 276, 281-

82 (1983) (holding police monitoring via beeper was not a search where suspect was only tracked on one particular trip to determine location of final destination).

The police conduct at issue in this case before the Court cannot be excused by the plain view doctrine, and thus the police were required to obtain a warrant prior to searching Leomund. Under the *Dunn* factors, Leomund's backyard is considered curtilage as it is near and adjacent to his home, enclosed by a wooded area at the back end of the property, used as a private meeting area, and had a second hidden entry so as to keep it hidden from those passing-by. J.A. at 15-16. Additionally, like the rural area in *Vargas*, Leomund's wooded backyard likely gave Leomund a heightened expectation of privacy. Leomund's backyard contained a table and shed, like the picnic table and gazebo in *Bagshaw*, which indicate that Leomund used his backyard for domestic purposes. J.A. at 16.

Leomund's backyard was not in the plain view of the officers who employed a drone to gather detailed and enhanced live-streamed images of the property and Leomund's activities. Unlike the marijuana plants in *Ciraolo*, Leomund's backyard and activities in his backyard were not viewable from a plane with the naked eye. Officer's needed to use the zoom feature on the camera to identify Leomund and Edgeworth and the map. J.A. at 16. While the pictures at issue in *Dow Chem. Co.* were later enhanced, in our case the camera's capabilities and the mobility of the drone led the officer's to move, pan, zoom, and focus all around Leomund's property, creating more than merely enhanced photos. J.A. at 25. Here, the officers utilized technology to provide much more information and many more images than an officer in a plane could have captured with his naked eye or even enhanced photographs. Additionally, as this Court noted in *Dow Chem. Co.*, the expectation of privacy is greater with outdoor areas on private property, as

opposed to commercial sites. Here, the observed area is adjacent to Leomund's home where he would expect heightened privacy rights.

Furthermore, this court has limited the use of technological devices to search in homes from outside the premises, and thus should do the same for curtilage. Just as this Court forbade the use of infrared devices to search inside a home from the outside in *Kyllo,* the use of a drone should likewise be prohibited. The drone enhanced the senses of the officers, similar to the way infrared enhances vision capabilities, such that they were able to gain detailed information and pictures that, without the technology, would have required a physical intrusion into the space. In *Karo,* this Court limited tracking devices when such devices informed police of something about the inside of the home. In much the same way, the drone revealed information to the officer's here about the activities of Leomund inside his backyard, which is akin to being inside his home. J.A. at 16. Unlike the suspect in *Knotts,* Leomund was tracked over multiple days and the monitoring was not limited to public travel destinations.

CONCLUSION

For the foregoing reasons, petitioner respectfully requests that the judgment of the United States Court of Appeals for the Fourteenth Circuit be reversed.