YOUR HARD DRIVE IS ALMOST FULL: HOW MUCH DATA CAN THE FOURTH AMENDMENT HOLD

Ismail Cem Kuru[*]

TABLE OF CONTENTS

* J.D. expected May 2016, University of Illinois College of Law, M.S. in Industrial Engineering, August 2013, Southern Illinois University Edwardsville. Thanks to the Honorable Cemil Kuru for being the beacon of my career. Many thanks to Andrew Leipold for teaching me the Fourth Amendment and his invaluable comments that contributed to this article. Thanks also to the editorial staff of the Illinois Journal of Law, Technology & Policy for all their hard work.

A tree falls down in a forest. If there is no one to hear it, does it make a sound? What if the tree falling down is your life being collected; your movement on public streets, your every phone call, your every visit to a website, and your every e-mail? What if that entity is the United States government? If the data is collected as a comprehensive record of United States history, saved on hard drives and it is never looked at, is that still an unreasonable search or seizure in violation of the Fourth Amendment of the United States Constitution? This article aims to answer that question.

Data collection is fundamentally different than data access.[1] Data collection, by itself, does not provide any information to the government.[2] Therefore, it makes sense to say that only when the data is processed and put in a logical form the government learns. This article argues that there is no search within the meaning of the Fourth Amendment when the government *collects* data. The search occurs when the government makes sense of the data by processing it through a computer, or by an individual government official or a law enforcement officer. The article further argues that a search warrant based upon probable cause is unreasonable because the mass collected data reveals much more than can be justified by the law enforcement interest. Finally this article proposes a preponderance of the evidence standard for access to collected data.

I. INTRODUCTION

Humankind has generated 90% of its data in the past two years.[3] This surge in data generation is, in part, a result of increase in electronic devices that seem to control our lives.[4] For example, upon using the Internet to view

1. ANDREW BLANN, DATA HANDLING AND ANALYSIS 2 (2015) ("[D]ata is effectively . . . information, and we use statistics to interpret this data—to make sense of and extract meaning from it.").

2. *See* Michael Pearson, *How Does U.S. Data Collection Affect Me?*, CNN POLITICS (June 9, 2013, 3:42 PM), http://www.cnn.com/2013/06/06/politics/nsa-verizon-records-questions/ (stating that the U.S. Government's policy is to not access collected records "without 'reasonable and articulable suspicion' that they're relevant to terrorist activity.").

3. Matthew Wall, *Big Data: Are You Ready for Blast-Off?*, BBC NEWS (Mar. 4, 2014), http://www.bbc.com/news/business-26383058 ("Some say that about 90% of all the data in the world today has been created in the past few years."); *What Is Big Data?*, IBM, http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html (last visited Mar. 9, 2016) ("Every day, we create 2.5 quintillion bytes of data—so much that 90% of the data in the world today has been created in the last two years alone.").

4. *See* George Simos, *How Much Data Is Generated Every Minute on Social Media*, WERSM (Aug. 19, 2015), http://wersm.com/how-much-data-is-generated-every-minute-on-social-media/ (illustrating the enormous amount of data generated on a per-minute basis through the use of social media sites by consumers

this article, you have generated many data points.[5] You presumably opened up a web browser; you entered a query to a search engine; identified this article as relating to your query; and viewed the article. All of those steps can be used to improve your life. The search engine might recognize your interest in the Fourth Amendment and show you relevant news, or it may show you articles with common characteristics to this one.

There are many advantages to utilizing these data sets. For example, the movie-streaming service Netflix utilizes data mining[6] to determine viewing habits of its subscribers.[7] With that knowledge, it can predict what movies you would like to watch next, or even what kind of shows it can develop.[8] Major online retailer Amazon.com uses similar techniques to suggest new items that may be interest to you based on your viewing and purchasing habits.[9]

The public perception of data seems to be linked to how much benefit it receives from that use. When the data is used in a way the public deems beneficial, such as the next movie to watch or what item to buy, such use is deemed acceptable.[10] Therefore when data is put to use for the individual's own benefit, the use is acceptable. Yet, website operators want to extract the entire benefit of such data by selling personally identifiable information to third parties,[11] and even governments.[12] Even if website operators do not sell

---

on their electronic devices).

5. *See Data, Data Everywhere*, ECONOMIST (Feb. 25, 2010), http://www.economist.com/node/15557443 (referencing the concept of "data exhaust"—the trail of data points created by internet users that can be analyzed to derive valuable information).

6. *What Is Data Mining (Predictive Analytics, Big Data)*, STATSOFT, http://www.statsoft.com/Textbook/Data-Mining-Techniques (last visited Mar. 6, 2016) ("Data Mining is an analytic process designed to explore data (usually large amounts of data—typically business or market related—also known as "big data") in search of consistent patterns and/or systematic relationships between variables, and then to validate the findings by applying the detected patterns to new subsets of data.").

7. Roberto Baldwin, *Netflix Gambles on Big Data to Become the HBO of Streaming*, WIRED (Nov. 29, 2012, 6:30 AM), http://www.wired.com/2012/11/netflix-data-gamble/.

8. *Id.*

9. Greg Linden et al., *Amazon.com Recommendations: Item-to-Item Collaborative Filtering*, IEEE INTERNET COMPUTING, Jan.–Feb. 2003, at 76, https://www.cs.umd.edu/~samir/498/Amazon-Recommendations.pdf; JP Mangalindan, *Amazon's Recommendation Secret*, FORTUNE (July 30, 2012, 11:09 AM), http://fortune.com/2012/07/30/amazons-recommendation-secret/.

10. Letter from Daniel Castro, Dir., Ctr. for Data Innovation, to Nicole Wong, Dep. Chief Tech. Officer, Office of Sci. and Tech. Policy (Mar. 31, 2014), http://www2.datainnovation.org/2014-ostp-big-data-cdi.pdf ("By helping individuals and organizations make better decisions, data has the potential to spur economic growth and improve quality of life in a broad array of fields."); Daniel Castro & Travis Korte, *Data Innovation 101: An Introduction to the Technologies and Policies Supporting Data-Driven Innovation*, CTR. FOR DATA INNOVATION (Nov. 4, 2013), http://www.datainnovation.org/2013/11/data-innovation-101/ ("Individuals use data to make better decisions about everything from what they buy to how they plan for the future."); *see also* Bernard Marr, *How Big Data Is Changing Healthcare*, FORBES (Apr. 21, 2015, 10:50 AM), http://www.forbes.com/sites/bernardmarr/2015/04/21/how-big-data-is-changing-healthcare/ (describing the benefits of data analysis in the context of the healthcare industry).

11. *See* Fred Guterl, *How Much Control Will We Have Over Our Personal Data?*, SCI. AM. (Jan. 25, 2015), http://blogs.scientificamerican.com/observations/2013/01/25/how-much-control-will-we-have-over-our-personal-data/ (describing the financial incentives companies have to monetize the valuable consumer data they have been collecting over the years and the related benefits that would be provided back to consumers by use of such data).

12. Bruce Schneier, *(Big) Brothers-in-Arms: The Global Public-Private Surveillance Partnership is as Strong as Ever*, BLAZE (Feb. 17, 2015, 9:00 AM), http://www.theblaze.com/blog/2015/02/17/the-global-public-private-surveillance-partnership-is-as-strong-as-ever/ ("Many countries use corporate surveillance capabilities to monitor their own citizens.").

the information directly, for example Google, which is an advertising company, generates most of its revenue from targeted ads.[13] A 2009 research report on user expectations on collected data suggests that there is "overwhelming concern by users about the collection of personal information and behavioral profiling."[14] The second concern of the user is the lack of control over the information collected and "for what purposes it may be used."[15]

The government can (and does) utilize data to improve our daily lives. In the most basic level traffic lights can be designed and coordinated in such a way to reduce average waiting times in intersections for both motor vehicles and pedestrians.[16] In the most complicated level, the National Security Agency (NSA) is collecting massive amounts of phone records without regards to any individualized suspicion for national security purposes.[17]

Big data analytics can revolutionize law enforcement with its ability to, "uncover hidden patterns, correlations, and other insights," in search for criminal activity.[18] Yet, we are reluctant to let government track our lives the same way as some private corporations.[19] With recent news of NSA surveillance, attentions turned to limiting and controlling the government's collection or use of our data.

The Framers could not have imagined the Internet and the possible uses and abuses of that remarkable technology. Yet, they did imagine the possible abuse of government's knowledge of our activities.[20]

The majority of the Supreme Court was wary of the question whether constant monitoring of a person's location through GPS, installed by law enforcement authorities on the criminal defendant's automobile without his knowledge, was a violation of the Fourth Amendment in *United States v. Jones*.[21] While the court ultimately held that such monitoring was a

13. MICHAEL H. MORRIS ET AL., CORPORATE ENTREPRENEURSHIP & INNOVATION 112 (2010) ("Google primarily generates revenue by delivering relevant, cost-effective online advertising.").

14. JOSHUA GOMEZ, TRAVIS PINNICK & ASHKAN SOLTANI, UC BERKELEY SCH. OF INFO., KNOWPRIVACY 17 (Oct. 10, 2009), http://escholarship.org/uc/item/9ss1m46b.

15. *Id.*

16. DDOT Blogger, *Signal Optimization and Improving Traffic Flow in the District*, D.ISH (Oct. 8, 2013), http://ddotdish.com/2013/10/08/signal-optimization-and-improving-traffic-flow-in-the-district/.

17. Matt Hamblen, *Snowden Leaks Furor Still Spilling Over Into Courts*, COMPUTERWORLD (Feb. 8, 2016, 12:02 PM), http://www.computerworld.com/article/3030661/data-privacy/ snowden-leaks-furor-still-spilling-over-into-courts-and-4th-amendment-debate.html; Dan Roberts & Spencer Ackerman, *Anger Swells After NSA Phone Records Court Order Revelations*, GUARDIAN (June 6, 2013, 9:05 PM), http://www.theguardian.com/world/2013/jun/06/obama-administration-nsa-verizon-records.

18. *Big Data Analytics: What It Is and Why It Matters*, SAS, http://www.sas.com/en_us/insights/analytics/big-data-analytics.html (last visited Mar. 9, 2016).

19. *See* Doug Aamoth, *PRISM Poll: Do You Care About the Government Mining Internet Data?*, TIME (June 7, 2013), http://techland.time.com/2013/06/07/prism-poll-do-you-care-about-the-government-mining-internet-data/ (indicating that consumers care about the government mining Internet data); *see also* John H. Fleming & Elizabeth Kampf, *Few Consumers Trust Companies to Keep Online Info Safe*, GALLUP (June 6, 2014), http://www.gallup.com/poll/171029/few-consumers-trust-companies-keep-online-info-safe.aspx (describing the lack of trust consumers have in companies with regards to keeping collected information secure).

20. *See* U.S. CONST. amend. IV (stating that the U.S. government's power to interfere with individuals' activities is limited—*i.e.*, by prohibiting "unreasonable searches and seizures. . . .").

21. United States v. Jones, 132 S. Ct. 945, 948 (2012).

"'search' within the meaning of the Fourth Amendment," they relied heavily on property-based trespass to decide the case.[22] Yet, Justice Alito, joined by three other justices, stated that they would decide the case under the *Katz* framework, and would find long-term monitoring of a person's location through GPS a violation of reasonable expectation of privacy.[23] Justice Sotomayor was the fifth vote in deciding the case under property-based trespass doctrine, yet she wrote a concurring opinion that went a step further than Justice Alito's opinion, stating that even short-term GPS monitoring could run afoul of the Fourth Amendment because it could reveal a lot of private information.[24]

If the Court eventually decides that constant GPS monitoring on public roads is a violation of the Fourth Amendment, it will open up a large avenue for litigators to argue the line that separates a violation and no violation.

Although GPS tracking is convenient and cost efficient, law enforcement does not need strict GPS tracking to know where you have been.[25] Our online presence creates enough data in various forms to allow an accurate picture of your life being drawn.[26] One particular example is the knowledge of location information to the cellular telephone companies.[27] When cell phones connect to the cell towers, the cell towers record the phone identification and the time of connection in each company's server, which can then be used to determine a rough travel route as the cell phone travels from tower to tower.[28]

There are two distinct points in the data collection process where the Fourth Amendment may potentially be implicated. The first point is when the information is initially gathered by the law enforcement agency. The acquisition can occur in many ways. For example, acquisition occurs when the traffic camera captures an image,[29] or when data is transmitted from a company such as Google or Facebook.[30] The acquisition of data is fundamentally different than seizure of property or person.[31] During the

22. *Id.* at 949.

23. *Id.* at 962, 964 (Alito, J., concurring).

24. *Id.* at 955 (Sotomayor, J., concurring).

25. *See* Kate Knibbs, *In the Online Hunt for Criminals, Social Media Is the Ultimate Snitch*, DIGITAL TRENDS (July 13, 2013), http://www.digitaltrends.com/social-media/the-new-inside-source-for-police-forces-social-networks/ (describing how law enforcement officers utilize social media to locate criminal suspects); *You Are Being Tracked*, ACLU, https://www.aclu.org/feature/you-are-being-tracked (last visited Mar. 9, 2016) (explaining how automatic license plate readers are utilized by U.S. law enforcement entities and private companies to track criminals and "to collect information about citizens' innocent activities just in case they do something wrong.").

26. Knibbs, *supra* note 25.

27. *See* In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (allowing the collection of cell site data under the third-party doctrine); Nathaniel Wackman, Note, *Historical Cellular Location Information and the Fourth Amendment*, 2015 U. ILL. L. REV. 263, 267 (2015) (describing "how police and prosecutors are using historical location data from cellular telephone companies to investigate and prosecute crimes.").

28. *See* Wackman, *supra* note 27, at 270–71 (explaining how cell service providers collect location and identification information through cell towers).

29. *Red Light Camera Enforcement*, CITY OF CHI., http://www.cityofchicago.org/city/en/depts/cdot/supp_info/red-light_cameraenforcement.html (last visited Mar. 9, 2016).

30. Sam Gustin, *Tech Titans Reveal New Data About NSA Snooping*, TIME (Feb. 3, 2014), http://time.com/3902/tech-titans-reveal-new-data-about-nsa-snooping/.

31. *See* Paul Ohm, *The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of*

acquisition of information, data is either created[32] or it is copied.[33] As will be explained further below, the acquisition does not fit well with the traditional definition of seizure with respect to the Fourth Amendment.

There are two issues to deal with when trying to analyze data collection using the traditional definition of seizure.[34] In many instances, search and seizure overlap in their protection.[35] Yet there is still a recognized distinction.[36] A search may occur when the privacy interest is implicated, such as listening to a conversation in a phone booth;[37] whereas seizure may occur when the possessory interest is implicated, such as the interest in freedom of movement.[38]

First of all, it is not clear whether there is any possessory interest in the data created on the Internet.[39] The Supreme Court, under the false friend doctrine, has addressed the situations where a third party collects information and then turns it over to law enforcement.[40] Similarly, "[d]ata in its ethereal, non-physical form is simply information."[41] The second issue is that there is no interference with the movement or freedom of the information flow.[42] Similar to wiretapping, data flow continues between the source and the

---

Intangible Property, 2008 STAN. TECH. L. REV. 40 (2008) (discussing the traditional definition of "seizure").

32. For example, a traffic camera creates a collection of data representing the image within its field of view. *Red Light Camera Enforcement*, *supra* note 29.

33. Although in common parlance it is spoken in terms of "turning over" the information to law enforcement agencies, only a copy of information is delivered, or more likely transmitted. *See* Gustin, *supra* note 30 (illustrating how companies "turn over" information to law enforcement agencies).

34. The seizure, as discussed below, occurs, "when the [law enforcement] officer, by means of physical force or show of authority, has in some way restrained the liberty of a citizen." Terry v. Ohio, 392 U.S. 1, 19 n.16 (1968). Similarly, a seizure of property occurs when there is, "some meaningful interference with an individual's possessory interests in that property." United States v. Jacobsen, 466 U.S. 109, 113 (1984).

35. J. SCOTT HARR ET AL., CONSTITUTIONAL LAW AND THE CRIMINAL JUSTICE SYSTEM 275 (6th ed., Cengage Learning 2015). For example, while prohibition against unreasonable searches protects your suitcase from being searched where it stands, prohibition against unreasonable seizures protects you by preventing the law enforcement with walking away with it.

36. Horton v. California, 496 U.S. 128, 133 (1990) ("A search compromises the individual interest in privacy; a seizure deprives the individual of dominion over his or her person or property."); *Jacobsen*, 466 U.S. at 113 ("A 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed. A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property."); *see also* Arizona v. Hicks, 480 U.S. 321 (1987) (holding that the police officer had seized stereo equipment when he moved it to record the serial numbers); Nicholas Poehl, *The Difference Between Search and Seizure*, AVVO (Sept. 1, 2011), http://www.avvo.com/legal-guides/ugc/the-difference-between-search-and-seizure (describing the distinction between the terms "search" and "seizure").

37. *Horton*, 496 U.S. at 133; Katz v. United States, 389 U.S. 347 (1967).

38. *Jacobsen*, 466 U.S. at 113.

39. *Id.* ("A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property."); *Horton*, 496 U.S. at 133 ("[A] seizure deprives the individual of dominion over his or her person or property."). The District Court that addressed NSA's data collection program considered both collection and use of the data as a search, and not a seizure. Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015).

40. *See, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979) (involving a telephone company turning over records to law enforcement officials); United States v. Miller, 425 U.S. 435 (1976) (involving a bank turning over records to law enforcement officials).

41. Digitech Image Techs., LLC v. Elecs. for Imaging, Inc., 758 F.3d 1344, 1350 (Fed. Cir. 2014).

42. United States v. Jones, 132 S. Ct. 945, 948 (2012) ("Indeed, the success of the surveillance technique that the officers employed was dependent on the fact that the GPS did not interfere in any way with the operation of the vehicle, for if any such interference had been detected, the device might have been discovered.").

destination, no one experiences any delays in phone conversations as the call is recorded or logged by phone companies.[43]

The second point in the data collection process where the Fourth Amendment may be implicated is when the information is accessed.[44] There are many reasons to access the collected information. The most obvious is identification of individuals.[45] For example, cities such as Baltimore, Chicago, and the District of Columbia have networks of video cameras surrounding areas where crime levels are higher, to identify individuals crimes.[46] A more "benign" reason for accessing such collected information may be for city development. For example, traffic engineering[47] relies on traffic volume in developing solutions to problems in city traffic networks.[48]

The purpose of this article is to devise a better way to frame the question of when a Fourth Amendment violation could occur with respect to technological surveillance, and subsequently analyze the legality of the use of data gathered by traffic cameras to monitor criminal activity.

II. METHODS OF COLLECTING AND ANALYZING INFORMATION

The Court never held that "potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment . . . . It is the exploitation of technological advances that implicates the Fourth Amendment, not their mere existence."[49] However, technological advances need to be understood before the implications of future law enforcement exploitations can be analyzed.

This section will discuss devices and methods that law enforcement agencies can utilize to gather and analyze information. There are two categories that involve fundamentally different prospects for violating privacy interests of individuals. First is direct data collection. These devices and methods involve a police enforcement agency actively creating a system that gathers information.[50] The second is indirect data collection. These involve data created for purposes other than law enforcement and are acquired, or that can be acquired, by the law enforcement agencies.[51]

---

43. *Klayman*, 957 F. Supp. 2d at 14. The details of mass data collection will be discussed further.

44. Throughout this Recent Development article, the terms "data analysis" and "data access" are used interchangeably.

45. Roberts & Ackerman, *supra* note 17. For example, if an agency has knowledge that a certain address is suspected of dealing contraband, the agency can also access GPS location data gathered through various sources to determine who have visited that location.

46. Andrea Noble, *D.C. Surveillance Cameras Become Top Crime-Fighting Tools for Police*, WASH. TIMES (June 30, 2013), http://www.washingtontimes.com/news/2013/jun/30/dc-surveillance-cameras-become-top-crime-fighting-/.

47. Traffic engineering is a branch of civil engineering that uses engineering techniques to achieve the safe and efficient movement of people and goods. ROGER P. ROESS ET AL., TRAFFIC ENGINEERING 160 (3d ed. 2004).

48. *Id.*

49. United States v. Karo, 468 U.S. 705, 712 (1984).

50. *Statistical Language—Data Sources*, AUSTL. BUREAU STAT. (last updated July 3, 2013), http://www.abs.gov.au/websitedbs/a3121120.nsf/home/statistical+language+-+data+sources.

51. *Id.*

A. Definitions

It is beneficial to start by defining several terms used throughout this Recent Development article.

"Data point" refers to the smallest piece of information collected.[52] For example, a traffic camera may record time and date, the license plate numbers of the vehicles that come in its view, speed of travel, location, or it may even take a picture.[53] Each of these recordings can be referred to as a data point. For example, time is one data point, and license plate number is also a data point. License plate number, removed from the rest of the information, does not reveal anything. Each of them by themselves are nearly meaningless.

"Data set" refers to a set of data points that have a meaningful relationship.[54] It consists of at least two data points and a meaningful relationship between them.[55] A license plate number by itself is meaningless, but when you combine a license plate number with a name and build a meaningful relationship between the two—ownership—you have something meaningful; that the individual owns a vehicle with the license plate number. For example, when the traffic camera records a license plate number, location, and traffic light condition, it would know that a vehicle with the license plate number has made a red light violation, if and only if the computer system is programmed to correlate the license plate number with the light condition.[56]

Take the opposite example where the system is not programmed to make such a correlation, and the camera simply records passing cars. Now, the data obtained by the camera has not yet created a meaning. The meaningful relationship is formed whenever a police officer reviews those tapes recorded by the camera and sees the red light, a vehicle passing the traffic stop line, and the license plate number.

Only by building relationships between data points can we obtain meaningful information. This relationship is necessary to understand the distinguishing principle between the fundamentally different actions between the acquisition of the information and access to that information. As it will be discussed in detail further below, at the acquisition stage data consists of a collection of data points with no meaningful relationship. When the data is accessed, however, meaningful relationships occur and consequently a search occurs.

B. Data Collection Techniques

Direct data collection is regarded as methods and devices that are more

52. NEW OXFORD AM. DICTIONARY 430 (2d ed. 2005).

53. *See* Gary L. Wickert & Melissa J. Fischer, *Big Brother's Eye in the Sky: Use of Red-Light Cameras in Accident Litigation*, CLAIMS J. (Aug. 7, 2014), http://www.claimsjournal.com/news/national/2014/08/07/252597.htm (explaining the functions and capabilities of traffic cameras).

54. NEW OXFORD AM. DICTIONARY, *supra* note 52.

55. *Id.*

56. Wickert & Fischer, *supra* note 53.

traditionally used by the law enforcement officers.[57] In particular, these are the methods where the law enforcement officer is taking an action that creates data.[58] Some of these devices have been around for a long time, such as wiretapping and video cameras.[59] Yet, especially with regards to video cameras, recent technological improvements allow more meaningful and efficient data processing, thereby allowing more effective use of these technologies.

1. Imaging

An image is a representation of what a human would see—it is the visual representation of light.[60] Most of the time, what we think of an image is an image representing the visible light. However, light is not limited to what we can see.[61] Infrared and radio are also forms of light.[62] What distinguishes them is their wavelength and human eyes' capability to detect them.[63] The map of all the types of light that we can identify comprises the electromagnetic spectrum.[64] The light classes are separated by wavelength, because the wavelength directly relates to how energetic the wave is.[65] Whether a particular wavelength passes through an object depends on the energy level of the light wave and the band gap of the atoms comprising the object.[66] While most solid objects reflect visible light, most allow the radio waves to pass through.[67]

Human ingenuity stepped up where human eyes have failed, and we have the capability to detect the entire spectrum of light.[68] Different devices and techniques are used for different light. The prices of such devices vary from $50 for a point-and-shoot camera to $15,000 for a gamma ray detector as the materials required to detect certain light is much more expensive than others.[69]

---

57. *See* Justine Brown, *Law Enforcement Agencies Face Complex Data Challenges*, GOV'T TECH. (July 20, 2015), http://www.govtech.com/data/Law-Enforcement-Agencies-Face-Complex-Data-Challenges.html (describing various ways police officers collect data, such as body camera footage, fingerprints, and surveillance video footage).

58. AUSTL. BUREAU STAT., *supra* note 50.

59. *History and Evolution of the Video Camera*, LIVEWATCH, https://www.livewatch.com/history-and-evolution-of-the-video-camera (last visited Mar. 9, 2016); William Lee Adams, *Brief History: Wiretapping*, TIME (Oct. 11, 2010), http://content.time.com/time/magazine/article/0,9171,2022653,00.html.

60. Valentin Dragoi, *Chapter 14: Visual Processing: Eye and Retina*, NEUROSCIENCE ONLINE (1997), http://neuroscience.uth.tmc.edu/s2/chapter14.html.

61. Molly Read, *Electromagnetic Spectrum*, U. WIS., http://cmb.physics.wisc.edu/pub/tutorial/spectrum.html (last visited Mar. 9, 2016).

62. *Id.*

63. *Id.*

64. *Id.*

65. *Id.* However, the categories that separate certain wavelengths are somewhat arbitrary and may overlap. For example, x-ray (generated by electrons in the atom) and gamma ray (generated by the nucleus in the atom) categories overlap at the high-energy boundary, and they are separated by their source.

66. *Wave Behaviors*, NASA.GOV, http://missionscience.nasa.gov/ems/03_behaviors.html (last visited Mar. 9, 2016).

67. *Id.*

68. Although this may be misleading since we only named the regions of electromagnetic spectrum that we can detect. Theoretically, the shortest wavelength can be as small as a marginally longer wavelength than the smallest particle of universe.

69. *See* HASTINGS A. SMITH, JR. & MARCIA LUCAS, LOS ALAMOS NAT'L LAB., PASSIVE

These technologies are commonplace. We are all familiar with movies where photographs of a suspect walking into a victim's home are found and shown at trial. Images document what is there, precisely. Although images can be altered,[70] these alterations can be detected.[71]

Fundamentally, what images do is provide information about a certain physical characteristic of the environment.[72] It provides that a certain light is being emitted or reflected by objects.[73] A camera shows the visible light, whereas a thermal imager shows the infrared light.[74] Only after an image is formed or information regarding the light is obtained, do we draw conclusions.

Further, each category of light gives us different information. If we detect that gamma ray radiation is radiating from a house, then we know there must be a radioactive material in the house because they do not occur naturally in the house.[75] Similarly, if we detect the infrared light coming from the house, then we can infer about the use of the house.[76] Unlike gamma rays, however, infrared light can tell us much more than just the existence of one particular type of material.[77]

a. Visible light

Although the history of cameras dates back to the sixteenth century, until the invention of photography—and the discovery that some substances are altered by exposure to light—in the early nineteenth century, there was no way to preserve the images.[78] What was once a costly and time-consuming endeavor is now a critical part of our culture. The number of photos uploaded and shared over the Internet has constantly risen since 2005, and in 2014, 1.8 billion photos were uploaded and shared per day.[79]

Cameras are most commonly used to capture visible light.[80] A digital

---

NONDESTRUCTIVE ASSAY MANUAL 63 (1991) (noting that higher resolution detectors are higher in cost in regard to gamma-ray detectors); *Gamma Ray Detectors*, EURSSEM, http://eurssem.eu/pages/c-4-3-gamma-ray-detectors (last visited Mar. 9, 2016); *Point & Shoot Digital Cameras*, AMAZON, http://www.amazon.com/s?rh=n%3A330405011%2Cp_36%3A1253504011 (last visited Mar. 9, 2016).

70. *See* President of the World, *Body Evolution—Model Before and After*, YOUTUBE (May 22, 2012), https://www.youtube.com/watch?v=17j5QzF3kqE&feature=youtu.be (showcasing an extreme example of how much photograph post-capture editing can affect the outcome).

71. *See, e.g.*, Alexy Kuznetsov et al., *Detecting Altered Images*, BELKASOFT (Aug. 22, 2013), https://belkasoft.com/detecting-forged-images (discussing how alterations to images can be detected).

72. *Chapter 2—Basic Theory—Electromagnetic Spectrum—Color is Reflected Light*, LIFEPIXEL, http://www.lifepixel.com/infrared-photography-primer/ch2-basic-theory-color-is-reflected-light (last visited Mar. 9, 2016).

73. *Id.*

74. *See Infrared Waves*, NASA, http://missionscience.nasa.gov/ems/07_infraredwaves.html (last visited Mar. 9, 2016) (noting thermal imaging technology that allows humans to perceive infrared light).

75. *See Gamma Rays*, NASA, http://missionscience.nasa.gov/ems/12_gammarays.html (last visited Mar. 9, 2016) (explaining that gamma waves on Earth emanate from radioactive material).

76. *See* NASA.GOV, *supra* note 74 (detailing how thermal imaging can be used to detect infrared waves emanating from any number of sources, including humans).

77. *See id.* (explaining that many objects emit infrared waves).

78. ROBERT HIRSCH, SEIZING THE LIGHT: A HISTORY OF PHOTOGRAPHY (2000).

79. Mary Meeker, *Internet Trends 2015—Code Conference*, KPCB (May 27, 2015), http://www.kpcb.com/internet-trends.

80. Jerry Lodriguss, *How Digital Cameras Work*, CATCHING THE LIGHT (2015),

camera includes a digital camera sensor.[81] The sensor, in turn, includes tiny light-sensitive diodes.[82] The light hitting the lens is directed to the sensor.[83] Light is a form of energy and each diode converts the energy in light into an electrical current.[84] This electrical current is then transferred into an analog-to-digital converter, which turns the signal from each diode into a digital value.[85] This digital value is the value for a pixel in the image.[86] The pixels are then combined to form an image.[87]

The major limitation in cameras is that the light must hit the lens. The camera records what it "sees." What the camera "sees" depends on the image sensor used.[88] Included in digital cameras commonly used by the public is an image sensor sensitive to visible light, which includes the wavelengths within 390 to 700 nanometers in the electromagnetic spectrum.[89]

b. Infrared Light

Infrared light has wavelengths longer than visible spectrum, from 700 nanometers to one millimeter.[90] By using diodes sensitive to infrared light wavelengths, images can be obtained with a camera.[91] Usually, false color is used to differentiate between objects emitting or reflecting higher and lower intensities of infrared light.[92] Thermal imagers use image sensors that are sensitive to infrared light.[93] Thermal imagers are useful in dark environments because every object that stores heat naturally emanates it as infrared light.[94] The increase in the temperature of the object increases the intensity of the infrared light.[95] Therefore, a difference in the temperature of adjacent objects allows the individual to distinguish between those objects, just like

http://www.astropix.com/html/i_astrop/how.htm.

81. There are two different digital camera sensors currently used, CMOS and CCD. GERALD C. HOLST & TERRENCE S. LOMHEIM, CMOS/CCD SENSORS AND CAMERA SYSTEMS (2d ed., JCD Publishing 2011); *see also* John Wenz, *These Simple Animations Show How Digital Camera Sensors Work*, POPULAR MECHANICS (May 8, 2015), http://www.popularmechanics.com/technology/a15436/heres-how-the-cmos-and-ccd-sensors-work/ (showing an animation of how this technology works).

82. Lodriguss, *supra* note 80.

83. *Id.*

84. *Id.*

85. *Id.*

86. *Id.*

87. *Id.*

88. *Imaging Electronics 101: Understanding Camera Sensors for Machine Vision Applications*, EDMUND OPTICS, http://www.edmundoptics.com/resources/application-notes/imaging/understanding-camera-sensors-for-machine-vision-applications/ (last visited Mar. 9, 2016).

89. *Id.*

90. *What Wavelength Goes with a Color?*, NASA, http://science-edu.larc.nasa.gov/EDDOCS/Wavelengths_for_Colors.html (last visited Mar. 9, 2016); *see also* JOHN AVISON, THE WORLD OF PHYSICS (2d ed. 2014).

91. Do Young Kim et al., *Multi-Spectral Imaging with Infrared Sensitive Organic Light Emitting Code*, NATURE (Aug. 5, 2014), http://www.nature.com/articles/srep05946#close.

92. Rhett Allain, *The World Looks Different Through an Infrared Camera*, WIRED (Apr. 9, 2014, 6:19 PM), http://www.wired.com/2014/04/the-world-looks-different-when-you-see-in-infrared/.

93. *Id.*

94. *Id.*

95. *Id.*

distinguishing between two objects emanating (or reflecting) visible light.[96] Although thermal imagers are much more expensive than the visible spectrum cameras, thermal imagers can now be purchased as an add-on for digital phones such as the iPhone.[97]

Night vision goggles also utilize infrared light, only at a lower wavelength and nearer to the visible spectrum.[98] An infrared light source positioned on the night vision goggle shines infrared light into the view of the user.[99] The goggles also include sensors capable of detecting infrared light reflected from nearby objects, and using false color based on intensity, the goggles show an image to the user.[100]

c. Radio Light

Radio waves are a form of light.[101] Radio waves include the wavelengths between one millimeter and 100 kilometers in the electromagnetic spectrum.[102] Radio waves can naturally be made by lightning or by astronomical objects.[103] Radio waves can be used to create images.[104] Further, objects in common use reflect radio waves just like any other light wave.[105] Because neither people or common household objects naturally emit radio waves, it is not possible to create an image of a closed enclosure, such as a house, from the radio waves emanating from inside the enclosure similar to thermal imagers.[106] However, it is possible to use a device to send radio waves with known wavelength and intensity, detect the reflected radio waves and determine whether a particular object, or person, is in the house,[107] or get an accurate "image" of the inside of

96. *Id.*

97. *See, e.g.*, FLIR ONE, http://www.flir.com/flirone/ (showing an example of an app-based thermal imager).

98. *Infrared Waves*, NASA, http://missionscience.nasa.gov/ems/07_infraredwaves.html (last visited Mar. 9, 2016).

99. Kendra Rand, *Infrared Light*, PHYSICS CENT., http://www.physicscentral.com/explore/action/infraredlight.cfm (last visited Mar. 9, 2016).

100. *How Night Vision Works*, SOFRADIR-EC, http://sofradir-ec.com/hownightvisionworks/ (last visited Mar. 6, 2016).

101. *Anatomy of an Electromagnetic Wave*, NASA, http://missionscience.nasa.gov/ems/02_anatomy.html (last visited Mar. 9, 2016).

102. CONCISE DICTIONARY OF SCI. 253 (2012).

103. *Id.*

104. Radar is the use of radio waves to detect objects. Emily Lakdawalla, *How Radio Telescopes Get "Images" of Asteroids*, PLANETARY SOC'Y (Nov. 8, 2011, 4:52 PM), http://www.planetary.org/blogs/emily-lakdawalla/2011/3248.html.

105. Ian Poole, *Electromagnetic Waves—Reflection, Refraction, Diffraction*, RADIO-ELECTRONICS.COM, http://www.radio-electronics.com/info/propagation/em_waves/electromagnetic-reflection-refraction-diffraction.php (last visited Mar. 9, 2016).

106. *Thermal Imaging: Facts vs. Fiction*, P&R INFRARED, http://pr-infrared.com/about-thermal-imaging/thermal-imaging-facts-vs-fiction/ (last visited Mar. 9, 2016).

107. As will be discussed later in this Recent Development article, the Tenth Circuit has addressed the use of such a device to determine if a suspect was inside the home before executing a search warrant. United States v. Denson, 775 F.3d 1214, 1219 (10th Cir. 2014) *cert. denied*, No. 14-9128, 2015 WL 1468640 (U.S. May 4, 2015); s*ee also* Brad Heath, *New Police Radars Can "See" Inside Homes*, USA TODAY (Jan. 20, 2015, 1:27 PM), http://www.usatoday.com/story/news/2015/01/19/police-radar-see-through-walls/22007615/ (suggesting at least fifty U.S. law enforcement agencies are utilizing radar devices to scout homes).

the enclosure by using several devices from different angles.[108]

2. Wiretapping

Wiretapping technology, even if it is newer than photography, is not new.[109] Wiretapping is authorized by a series of federal and state statutes.[110] Wiretapping is a broad term, which encompasses many methods of intercepting communications. It receives its name because in the days of landline phones, the wires that composed the landline needed to be altered to redirect signals traveling along the wire to another location.[111]

Yet, it is possible to "wiretap" without physical intrusion. Communications over radios can be "tapped" using a radio frequency receiver operating at the same frequency as the radios.[112] There are technical—even if not conceptual—differences in the tapping method based on the technology being used. Further, in the context of communications through the Internet, there are many points between the communication initiator and the intended recipient where a communication can be intercepted, recorded, or copied.

To illustrate these concepts, take for example, an e-mail communication between Jack and Sally. Jack types the e-mail address into his browser. Whatever is typed on a computer can be recorded and transmitted to a third party using specialized software called a keylogger.[113] The e-mail either travels to a wireless router using radio waves over the air or to a wired router using electrical current over an ethernet cable.[114] Radio waves can be obtained using an appropriate radio receiver operating at the same frequency.[115] Wires can be tapped by intercepting the electrical current during its travel.[116] Next, the router sends data representing the e-mail to an Internet Service Provider ("ISP") using fiber optic cables.[117] Fiber optic cables are hollow tubes that are

---

108. This technique is similar to a CAT scan in a hospital, which uses hundreds of x-ray scans from different angles to create a 3D image of the tissue. *Computed Tomography (CT)—Body*, RADIOLOGYINFO.ORG (Sept. 23, 2014), http://www.radiologyinfo.org/en/info.cfm?pg=bodyct.

109. William Lee Adams, *Brief History: Wiretapping*, TIME (Oct. 11, 2010), http://content.time.com/time/magazine/article/0,9171,2022653,00.html.

110. *See* ADMIN. OFFICE OF U.S. COURTS, WIRETAP REPORT 2013, TABLE 1 (2013), http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2013/Table1.pdf (listing jurisdictions with statutes authorizing wiretapping activities).

111. *See* R. SHIREY, IETF TRUST, INTERNET SECURITY GLOSSARY 336 (2d rev., Aug. 2007), http://tools.ietf.org/html/rfc4949 (stating that "[a]lthough the term originally referred to making a mechanical connection to an electrical conductor that links two nodes, it is now used to refer to accessing information from any sort of medium used for a link or even from a node, such as a gateway or subnetwork switch.").

112. Radio waves can be captured with any radio receiver device configured to the same frequency as the radio wave. *Catch a Wave: Radio Waves and How They Work*, ILLUMIN [hereinafter *Catch a Wave*], http://illumin.usc.edu/114/catch-a-wave-radio-waves-and-how-they-work/ (last visited Mar. 6, 2016).

113. Nikolay Grebennikov, *Keyloggers: How They Work and How to Detect Them*, SECURELIST (Mar. 29, 2007, 1:03 PM), https://securelist.com/analysis/publications/36138/keyloggers-how-they-work-and-how-to-detect-them-part-1/.

114. *How Does Wirelesss Internet Work*, WIRELESS TECH. ADVISOR, http://www.wireless-technology-advisor.com/how-does-wireless-internet-work.html (last visited Mar. 9, 2016).

115. *Catch a Wave*, *supra* note 112.

116. *Fact Sheet 9: Wiretapping and Eavesdropping on Telephone Calls*, PRIVACY RTS. CLEARINGHOUSE, (Feb. 2016), https://www.privacyrights.org/content/wiretapping-and-eavesdropping-telephone-calls.

117. *Exploring the Modern Computer Network: Types, Functions, and Hardware*, CISCO (Dec. 19, 2013), http://www.ciscopress.com/articles/article.asp?p=2158215&seqNum=6.

covered with reflective coating, and information is carried using light.[118] It is possible with a technique not unlike wiretapping to direct some of the light traveling through fiber optic cable to a third location and extract information.[119] The ISP receives the e-mail in a local Point of Presence server. It then redirects the e-mail to an Internet Exchange Point ("IXP") server.[120] Each IXP server connects many ISP servers, and each IXP server is connected to one or more other IXP servers.[121] Every time the e-mail reaches an ISP Point of Presence server or an IXP server, it is stored briefly in a data center.[122] Whatever data is stored in the IXP can be copied to a secondary data center without affecting the journey of e-mail from Jack and Sally.[123] In fact, most e-mail servers (Google, Microsoft, Yahoo, etc.) store a copy of the e-mail on their computer.[124] The e-mail then follows a similar path—ISP, router, computer—to reach Sally's browser.[125]

Now that we know where the information can be copied, we can continue to discuss how this is accomplished.

3. Keyloggers

Computers can be tapped by installing specialized software called a "keylogger."[126] Keyloggers record every keystroke made by the user of the computer on which it is installed.[127] They can also be programmed to transmit the collected data to another computer when it is connected to a network or Internet.[128] Although it is generally used for criminal purposes, or spying on

118. Information transferred using light is faster because light travels faster than electrical current and there is less resistance (therefore less loss of power) along the travel. *How Fiber-Optic Internet Works*, BEACON, http://fios.verizon.com/beacon/how-fiber-optic-internet-works/ (last visited Mar. 9, 2016).

119. U.S. Patent No. 6,535,671 (filed Feb. 27, 2001); *see also* KIMBERLIE WITCHER, FIBER OPTICS AND ITS SECURITY VULNERABILITIES 8 (Feb. 17, 2005), https://www.sans.org/reading-room/whitepapers/physical/fiber-optics-security-vulnerabilities-1648 (stating that "[t]o do a virtually undetected tap, it is almost certain that intruders would only need available commercial items, such as, a laptop, optical tap, packet-sniffer software, and an optical/electrical converter.").

120. *What Is an Internet Exchange Point?*, NETNOT https://www.netnod.se/ix/what-is-ixp (last visited Mar. 9, 2016) [hereinafter *What Is an IXP?*].

121. *See generally* PATRICK S. RYAN & JASON GERSON, A PRIMER ON INTERNET EXCHANGE POINTS FOR POLICYMAKERS AND NON-ENGINEERS (Aug. 11, 2012), http://ssrn.com/abstract=2128103 (describing the architecture of IXP servers and systems).

122. *What Is an IXP?*, *supra* note 120.

123. *See generally*, INTERNET SOC'Y, THE INTERNET EXCHANGE POINT TOOLKIT & BEST PRACTICES GUIDE (Feb. 2014), https://www.internetsociety.org/sites/default/files/Global%20IXPToolkit_Collaborative%20Draft_Feb%2024.pdf (summarizing IXP distribution protocols).

124. *See, e.g.*, Benjamin Mako Hill, *I Don't Use Gmail, but Google Still Has Lots of My Personal Emails*, SLATE (May 13, 2014, 2:03 PM), http://www.slate.com/blogs/future_tense/2014/05/13/don_t_use_gmail_here_s_how_to_determine_how_many_of_your_emails_google_may.html (discussing Google servers storing copies of sent and received e-mails).

125. *See* J. KLENSIN, INTERNET SOC'Y, SIMPLE MAIL TRANSFER PROTOCOL (Apr. 2001), http://www.ietf.org/rfc/rfc2821.txt (showing a simple e-mail transfer protocol); s*ee also* JONATHAN B. POSTEL, UNIV. S. CAL. INFO. SCI. INST., SIMPLE MAIL TRANSFER PROTOCOL (Aug. 1982), http://www.ietf.org/rfc/rfc821.txt (showing a simple mail transfer protocol example).

126. *See* OXFORD ONLINE DICTIONARY, http://www.oxforddictionaries.com/definition/english/keylogger (last visited Mar. 9, 2016) (providing the definition of "keylogger").

127. Grebennikov, *supra* note 113.

128. *Id.*

friends' and families' Facebook accounts,[129] it can also be used to gather information about suspects' activities on the computer by gathering screenshots in addition to keystrokes.

One method of delivering a keylogger to a computer is by using a Trojan horse.[130] A Trojan horse is harmful software depicted as useful.[131] These can be planted on websites flagged as dangerous, such as a website used in dissemination of child pornography, or a website belonging to a known criminal organization.[132] A user visiting the website is asked to download a software to his computer depicting it as a helpful tool, or as the content the user is looking for.[133] Once a computer user tries to open the software, nothing happens on the screen.[134] The program starts recording and transmitting the information to a police officer or a third party to be analyzed.[135]

Smart phones are essentially a small computer, and therefore they can also be tapped using keyloggers.[136]

4. Radio Signals

Radio signals are a form of light with wavelengths ranging from one millimeter to 100 kilometers.[137] Radio signals are potentially the easiest to capture because they travel over the air and reception of the signal at one receiver does not affect the transmission of the signal to its intended destination.[138] Both wireless Internet and cell phones operate over the air using radio frequency signals.[139]

Cell phones use radio signals to communicate with the cell towers.[140]

---

129. *Security Spotlight: A Closer Look at Malicious Keyloggers*, IOLO, http://www.iolo.com/resources/articles/security-spotlight-a-closer-look-at-malicious-keyloggers/ (last visited Mar. 9, 2016).

130. Mary Landesman, *What Is a Keylogger Trojan?*, ABOUT TECH, http://antivirus.about.com/od/whatisavirus/a/keylogger.htm (last visited Mar. 9, 2016).

131. *Id.*

132. *What is a Keylogger Virus and How to Remove It*, COMBOFIX (Feb. 13, 2012), http://www.combofix.org/what-is-a-keylogger-virus-and-how-to-remove-it.php; *see also Trojan Virus Used to Monitor Criminals in Germany*, DW NEWS (Oct. 19, 2011), http://www.dw.com/en/trojan-virus-used-to-monitor-criminals-in-germany/av-6641838 (showing a video of the German Justice Minister detailing a policy that uses Trojans to monitor convicted criminals on the Internet).

133. Pieter Arntz, *What are Trojans?*, MALWAREBYTES LABS (June 4, 2013), https://blog.malwarebytes.org/intelligence/2013/06/what-are-trojans/.

134. *Id.*

135. The courts have not yet resolved the legality of wiretapping under the Fourth Amendment. The courts that have looked at wiretapping did so in the context of the Federal Wiretap Act, 18 U.S.C. §§ 2510–2522 (2012). *See, e.g.*, Halperin v. Int'l Web Servs. LLC, 70 F.Supp.3d 893, 901–03 (N.D. Ill. 2014) (examining allegations of wiretapping in the context of the Federal Wiretap Act).

136. *See, e.g.*, *iKeyMonitor—Best Android Keylogger*, IKEYMONITOR, http://ikeymonitor.com/android-keylogger (describing and selling an app used to log Android phone activities) (last visited Mar. 9, 2016).

137. CONCISE DICTIONARY OF SCIENCE, *supra* note 102.

138. STEFAAN SEYS & BART PRENEEL, ARM: ANONYMOUS ROUTING PROTOCOL FOR MOBILE AD HOC NETWORKS (2006) (discussing why the nature of radio transmissions makes them easier to capture). As an example, consider the situation where you can turn on two television sets with the same remote at the same time.

139. Marshall Brian et al., *How WiFi Works*, HOWSTUFFWORKS (Apr. 30, 2001), http://computer.howstuffworks.com/wireless-network1.htmhttp://computer.howstuffworks.com/wireless-network1.htm.

140. *Id.*

Cell towers broadcast radio signals in frequent intervals.[141] When a cell phone comes in the cell tower range, it replies to the tower with an authentication code.[142] If the tower approves the authentication code, a connection is made.[143] At any given time, a cell phone can be in communication with several towers simultaneously.[144] The frequency of the radio signal depends on the carrier[145] and is regulated by the Federal Communications Commission.[146]

Cell phone signals can be intercepted as they travel through the air using any receiver operating at the same frequency[147] because the cell phone broadcasts the signal in every direction—it does not have the capability, nor the necessity, to broadcast the signal in a particular direction.[148] The information contained in the radio signals is compressed and encrypted by the wireless communication companies.[149] Yet, these encryptions are not safe.[150] Therefore, it is possible to listen in to a phone conversation with relative ease.

One device created specifically for this purpose is commonly called a Stingray.[151] A Stingray device acts as a pirate cell tower.[152] It broadcasts signals similar to that of a legitimate cell tower.[153] The signal strength gradually increases.[154] Because cell phones are programmed to connect to the

141. Michael Harris, *How Cell Towers Work*, UNISON (Mar. 9, 2011), http://www.unisonsite.com/resource-center/resource.html?article=40 ("The primary job of a cell tower is to elevate antennas that transmit and receive radio-frequency (RF) signals from mobile phones and devices.").

142. *Cell-Phone Technology*, WIKIEDUCATOR.ORG, https://wikieducator.org/images/7/7f/Cell_Phone_technology.pdf (last visited Mar. 9, 2016).

143. *Id.*

144. Marguerite Reardon, *Turning Cell Phones into Lifelines*, CNET.COM (Dec. 8, 2006), http://www.cnet.com/news/turning-cell-phones-into-lifelines/ (illustrating that through mobile switching centers, cell phones can be connected to multiple towers).

145. *Frequencies by Provider*, WILSONAMPLIFIERS (Oct. 12, 2014), http://www.wilsonamplifiers.com/frequencies-by-provider.

146. 47 C.F.R. § 2.106 (2014); *Radio Spectrum Allocation*, FCC, https://www.fcc.gov/encyclopedia/radio-spectrum-allocation (last visited Mar. 9, 2016).

147. *Police Use Stingray Tool to Intercept Cellphone Signals*, NAT'L PUBLIC RADIO (Aug. 4, 2015), http://www.npr.org/2015/06/22/416538036/police-use-stingray-tool-to-intercept-cell-phone-signals (illustrating that certain types of equipment can intercept radio signals over the air).

148. Clay Dillow, *By "Beamsteering" Antenna Signals in One Direction, Devices' Power Consumption Could Be Halved*, POPULAR SCI. (Dec. 15, 2010), http://www.popsci.com/technology/article/2010-12/steering-mobile-device-signals-one-direction-power-consumption-could-be-halved.

149. *The Cell Phone Technology*, U.C. SANTA BARBARA, http://www.mat.ucsb.edu/~g.legrady/academic/courses/03w200a/projects/wireless/cell_technology.htm (last visited Mar. 9, 2016).

150. "Speaking at the Chaos Computer Club (CCC) Congress in Berlin on Tuesday, a pair of researchers demonstrated a start-to-finish means of eavesdropping on encrypted GSM cellphone calls and text messages, using only four sub-$15 telephones as network 'sniffers,' a laptop computer, and a variety of open source software." Jon Borland, *$15 Phone, 3 Minutes All That's Needed to Eavesdrop on GSM Call*, ARS TECHNICA (Dec. 29, 2010, 8:58 AM), http://arstechnica.com/gadgets/2010/12/15-phone-3-minutes-all-thats-needed-to-eavesdrop-on-gsm-call/.

151. Joel Hruska, *Stingray, the Fake Cell Phone Tower Cops and Carriers Use to Track Your Every Move*, EXTREMETECH (June 17, 2014, 4:51 PM), http://www.extremetech.com/mobile/184597-stingray-the-fake-cell-phone-tower-cops-and-providers-use-to-track-your-every-move.

152. *Id.*

153. *Id.*

154. *The Cell Phone Technology*, U.C. SANTA BARBARA, http://www.mat.ucsb.edu/~g.legrady/academic/courses/03w200a/projects/wireless/cell_technology.htm (last visited Mar. 20, 2016); *Cellular Handover and handoff*, RADIO-ELECTORNICS.COM, http://www.radio-electronics.com/info/cellulartelecomms/cellular_concepts/handover_handoff.php (last visited Mar. 20, 2016).

cell tower with the highest signal strength, when the signal from a Stingray reaches a critical point, nearby cell phones connect to the Stingray rather than the legitimate cell tower.[155]

A Stingray at this point acts as a bridge between the cell phone and the cell tower.[156] It broadcasts signals to the nearby cell towers with the device identification of those devices that are connected to it.[157] When a Stingray communicates with the cell tower, it conceals itself and acts as the cell phone would (with the cell phone's identification and registration codes that it received when the cell phone tried to register with the Stingray), receives any incoming information from the cell tower and stores it before transmitting it to the cell phone.[158] Similarly, any information—the device identification, phone numbers, text messages—sent from the cell phone passes through the Stingray and can be recorded at the Stingray before being transmitted to the cell tower or vice versa.[159]

The capabilities of a Stingray do not end there however. It can manipulate the transmissions to and from the cell tower or block them completely; instead of sending a transmission as soon as it receives it, it can store it.[160] Then the user of the device can manipulate the transmission, such as the contents of a text message, and continue to transmit it to the cell tower when the modification is completed.[161]

5. Global Positioning System (GPS) Devices

GPS is a network of satellites that are positioned around Earth, which allows for determining the position of a GPS device on Earth. Initially developed as a military project, GPS uses radio waves to triangulate[162] the position of the receiver. Each GPS satellite broadcasts its position and the current time at regular intervals.[163] When a GPS receiver is activated it searches for signals from GPS satellites that are broadcasted on two frequencies.[164] The receiver uses this information to calculate its position on

155. Kate Martin, *Documents: Tacoma Police Using Surveillance Device to Sweep Up Cellphone Data*, NEWS TRIBUNE (Aug. 26, 2014, 3:56 PM), http://www.thenewstribune.com/news/local/article25878184.html.

156. *Id.*

157. *Id.*

158. *Id.*

159. Clarence Walker, *New Hi-Tech Police Surveillance: The "StingRay" Cell Phone Spying Device*, GLOBALRESEARCH (May 19, 2015), http://www.globalresearch.ca/new-hi-tech-police-surveillance-the-stingray-cell-phone-spying-device/5331165 (discussing the data capturing capabilities of the StingRay device).

160. *Id.*

161. Hanni Fakhoury & Travor Timm, *Stingrays: The Biggest Technological Threat to Cell Phone Privacy You Don't Know About*, ELEC. FRONTIER FOUND. (Oct. 22, 2012), https://www.eff.org/deeplinks/2012/10/stingrays-biggest-unknown-technological-threat-cell-phone-privacy.

162. TIM STOMBAUGH ET AL., UNIV. KY. COLL. OF AGRIC., GPS SIMPLIFIED (2002), http://www2.ca.uky.edu/agc/pubs/pa/pa5/PA5.PDF (discussing triangulation, a common method for determining the location of a radio receiver using three or more signals of known origin and transmission time).

163. *How Does GPS Work?*, PHYSICS.ORG, http://www.physics.org/article-questions.asp?id=55 (last visited Mar. 9, 2016).

164. *Introduction to GPS*, ESRI, http://webhelp.esri.com/arcpad/8.0/userguide/index.htm#capture_devices/concept_intro.htm (last visited Mar. 9, 2016).

Earth using a method called triangulation.[165]

The waves broadcasted by the GPS satellites are radio waves, which means that they are a form of light and travel at the speed of light.[166] When the receiver receives a signal, it learns where the satellite is and when it sent the signal.[167] The receiver also includes a clock.[168] Therefore, the receiver knows how long it took the wave from the satellite to arrive at its location.[169] A basic principle of physics is that velocity multiplied by time equals distance.[170] The receiver thus knows that it is somewhere within a certain distance from a particular location—the location of the satellite when it broadcasts.[171] The receiver repeats the same process twice for waves from two other satellites.[172] These calculations give the receiver three intersecting spheres.[173] There will be several points where all three spheres intersect.[174] All but one will suggest that the receiver is far away from Earth's surface; therefore they can be discarded.[175] The remaining location is the location of the receiver.[176]

The GPS device does not transmit any information to the satellite in order to calculate its location; this is done internally on the device.[177] The device that encompasses the GPS receiver, such as a smart phone, has other capabilities—Wi-Fi, Bluetooth, and radio transmitter to connect to the cell tower—that can broadcast its location.[178]

Since there is no requirement of transmitting any signal to the GPS satellite, the GPS satellite does not store any information regarding how many devices or the identification of devices in its system.[179] Therefore, the only way to determine the location of a cell phone with a GPS device is if the cell phone broadcasts its location.

6. Fiber Optic Tapping

As briefly articulated above, fiber optic cables can be tapped just as easily as landlines could. Fiber optic cables are coated inside with light reflective

165. STOMBAUGH, *supra* note 162.
166. XU GUOCHANG, GPS: THEORY, ALGORITHMS AND APPLICATIONS 87 (2d ed. 2007).
167. *Id.* at 3.
168. *Id.* at 204.
169. *Id.* at 3.
170. *Speed and Velocity*, PHYSICS CLASSROOM, http://www.physicsclassroom.com/class/1DKin/Lesson-1/Speed-and-Velocity (last visited Mar. 9, 2016).
171. GUOCHANG, *supra* note 166.
172. *Id.* at 108.
173. *Id.* at 53.
174. *Id.*
175. *Id.* at 183
176. *Id.*
177. *Id.* at 3.
178. Guy McDowell, *How Do Satellites Track Mobile Phones? [Technology Explained]*, MAKEUSEOF (Aug. 8, 2009), http://www.makeuseof.com/tag/technology-explained-how-do-satellites-track-mobile-phones/ (illustrating that GPS-enabled phones broadcast their signals in order to be tracked).
179. *Cellular vs. Satellite: Understanding the Differences*, GLOBAL DATA SYSTEMS (Feb. 24, 2015, 9:42 AM), http://www.getgds.com/blog/cellular-vs.-satellite-understanding-the-differences (explaining that cell phones use land-based towers and do not communicate with satellites directly).

material and commonly used to transmit internet flow.[180] The light transmits data at a much higher speed and with less loss in power during transmission.[181] Unlike copper wires that have resistance to the electrical current carrying data, air inside fiber optic cable applies little to no resistance to the light.[182] Further, light has a certain energy level. To ensure that light reaches its destination, energy used in transmission is higher than necessary.[183] A portion of the light can be redirected from its path without loss of any data transmission.[184] The energy level reaching the destination will be less because some of it is redirected, but the information will be transmitted regardless.[185]

Most of the data flowing between ISPs are transferred using fiber optic cables.[186] Fiber optic cables have higher bandwidth, so they can carry more data than copper cables, which is the type of cable used by the cable companies.[187]

7. Data copying

The easiest way to gather data is by copying. In the common parlance, when we talk about an e-mail being "sent," the data that shows the e-mail on your computer in fact stays in your computer until a copy of it is transmitted through the communication medium, and then it is deleted from your computer; nothing physical actually leaves the computer.[188] The Internet is a network of networks. It includes many storage units connected in networks of storage units, which are connected with other networks creating a massive world wide web of storage units.[189] Internet Exchange Points ("IXP") are some of the more centralized locations where Internet traffic flows.[190] Some of the more important IXPs are the ones connecting the United States to Asia and Europe.[191] When IXPs receive data, the data is temporarily stored in the data

180. *Physics of Total Internal Reflection*, HOWSTUFFWORKS, http://computer.howstuffworks.com/fiber-optic6.htm (last visited Mar. 9, 2016).

181. Miguel Leiva-Gomez, *MTE Answers: Why Is Fiber Optic Internet Faster Than Copper?*, MAKETECHEASIER.COM (July 14, 2014), https://www.maketecheasier.com/why-is-fiber-optic-internet-faster-than-copper/.

182. *Id.*

183. *Introduction to Optical Fibers, dB, Attenuation and Measurements*, CISCO, http://www.cisco.com/c/en/us/support/docs/optical/synchronous-digital-hierarchy-sdh/29000-db-29000.html (noting that excess energy is lost until fiber reaches equilibrium) (last visited Mar. 9, 2016).

184. Vivek Alwayn, *Fiber-Optic Technologies*, CISCO (Apr. 23, 2004) http://www.ciscopress.com/articles/article.asp?p=170740&seqNum=3 (noting that if "the angle of incidence is always equal to the angle of reflection, the reflected light continues to be reflected.").

185. CORNING, GET THE FACTS ON OPTICAL FIBER! (2012), http://media.corning.com/flash/opticalfiber/2012/corning_optical_fiber/Documentation/FIBER_MATTERS/flipbook/585324499/files/inc/585324499.pdf (last visited Mar. 9, 2016).

186. *Id.*

187. *Id.*

188. *See* Dan Gookin, *How E-Mail Works*, FOR DUMMIES, http://www.dummies.com/how-to/content/how-email-works.html (describing, very basically, how e-mail is transferred between recipients) (last visited Mar. 9, 2016).

189. INT'L TELECOMM. UNION, INTERNET EXCHANGE POINTS (IXPS), (Mar. 2013), https://www.itu.int/en/wtpf-13/Documents/backgrounder-wtpf-13-ixps-en.pdf.

190. *Id.*

191. Dennis Weller & Bill Woodcock, *Internet Traffic Exchange: Market Developments and Policy Changes*, OECD DIG. ECON. PAPERS (2013), http://www.oecd-ilibrary.org/science-and-technology/ internet-

center before being sent to another IXP.[192] Because of the volume of data flowing through IXPs, this temporary storage is quickly deleted.[193] Yet until it is deleted, it is susceptible to being copied.[194]

C. Data Processing Methods

Any data gathered through a device must be processed one way or another. A microchip on the digital camera analyzes the electrical signals from the light sensor in the camera to create the image that was captured.[195] The microchip in the camera can do this very simply because the data incoming from the sensor is structured.[196] This means that there is an order to the information stream, and it is in a known format.[197] Other forms of data collection may have similar ordered structures making it easy to discern meaning from them.

The real source of information for law enforcement purposes is the Internet. As commentators[198] and news media[199] recognize, much of our personal information is publicly available online. In a very inspiring and concerning way, Alessandro Acquisti shares that from a picture of a random person, you can reach his social security number in two steps using publicly shared information.[200] The major difficulty with the information available on the Internet is that most of the data is unstructured.[201] The unstructured data is more difficult to analyze because as its name suggests, it does not have a particular order.[202]

Yet, big data analytics is a growing field, and it is continuing to improve the way we view data.[203] Also called data mining,[204] data processing methods

---

traffic-exchange_5k918gpt130q-en.

192. GREG PANGRAZIO, SANS INSTITUTE, INTEL IXP NETWORK PROCESSOR BASED INTRUSION DETECTION (May 22, 2007), https://www.sans.org/reading-room/whitepapers/detection/intel-ixp-network-processor-based-intrusion-detection-32919.

193. *Id.*

194. *Id.*

195. Kyle Schurman, *How Does a Digital Camera Work?*, GADGET REV., http://www.gadgetreview.com/how-does-a-digital-camera-work (last visited Mar. 9, 2016).

196. *See id.* (explaining how digital cameras take photographs, digitize them, and create files to view later).

197. *Id.*

198. *See, e.g.*, Jose Felipe Anderson, *Big Brother or Little Brother? Surrendering Seizure Privacy for the Benefits of Communication Technology*, 81 MISS. L.J. 895, 911 (2012) ("The average citizen has lost so much control over their personal information that it may be impossible to reverse the trend.").

199. *E.g.*, Jacob Morgan, *Privacy Is Completely and Utterly Dead, and We Killed It*, FORBES (Aug. 19, 2014, 12:04 AM), http://www.forbes.com/sites/jacobmorgan/2014/08/19/privacy-is-completely-and-utterly-dead-and-we-killed-it/.

200. Alessandra Acquisti, *What Will a Future Without Secrets Look Like?*, TED (June 2013), http://www.ted.com/talks/alessandro_acquisti_why_privacy_matters.

201. RONEN FELDMAN & JAMES SANGER, THE TEXT MINING HANDBOOK: ADVANCED APPROACHES IN ANALYZING UNSTRUCTURED DATA (2006).

202. WILLIAM H. INMON & ANTHONY NESAVICH, TAPPING INTO UNSTRUCTURED DATA: INTEGRATING UNSTRUCTURED DATA AND TEXTUAL ANALYTICS INTO BUSINESS INTELLIGENCE (2007).

203. *See* Molly Galetto, *Machine Learning and Big Data Analytics: The Perfect Marriage*, NG DATA, http://www.ngdata.com/machine-learning-and-big-data-analytics-the-perfect-marriage/ (last updated Feb. 26, 2016) (describing the field known as "Big Data" and the challenges posed to data analytics).

204. 1 WAYNE R. LAFAVE, SEARCH & SEIZURE § 2.7(e) (5th ed. 2012).

uncover the secret meaning in seemingly unrelated data.[205]

One of the most innovative data mining techniques is the use of machine learning algorithms.[206] Traditionally, a computer program would do exactly what has been programmed, and every step of the analytical rule needed to be written in the program.[207] Machine learning algorithms on the other hand, generalize analytical rules from examples.[208] It saves tremendous amount of time in data analysis.[209]

III. BACKGROUND AND ANALYSIS

A. Text of the Fourth Amendment

The Fourth Amendment of the United States Constitution has its roots, much like many other parts of the U.S. Constitution, in English traditions disliked by the colonies.[210] Yet, the Fourth Amendment reflects the most direct attempt to protect against "writs of assistance."[211] These general warrants allowed officers of the King of England to enter any home and seize any item that they considered contraband.[212]

Although the courts in England considered the practice of general warrants illegal,[213] the practice was continued by English authorities in the colonies to search for evidence of smuggling activities.[214]

The Fourth Amendment to the United States Constitution states:

> 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.[215]

The first half of the Fourth Amendment bans "unreasonable searches and seizures."[216] The second half, known as the Warrant Clause, prohibits issuance of warrants without probable cause and requires particularity in its

205. Note, *Data Mining, Dog Sniffs, and the Fourth Amendment*, 128 HARV. L. REV. 691 (2014).

206. Galetto, *supra* note 203.

207. Guy M. Haas, *Introduction to Computer Programming*, BFOIT, http://www.bfoit.org/itp/Programming.html (last visited Mar. 9, 2016).

208. Pedro Domingos, *A Few Useful Things to Know About Machine Learning*, 55 COMMS. ACM 78 (Oct. 2012), http://homes.cs.washington.edu/~pedrod/papers/cacm12.pdf.

209. *See, e.g.*, Sneha Agarwal et al., *Patci—A Tool for Identifying Scientific Articles Cited by Patents*, GSLIS RESEARCH SHOWCASE (Mar. 14, 2014), https://www.ideals.illinois.edu/handle/2142/54885 (showing a successful machine learning algorithm to populate fields from unstructured textual data).

210. Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979 (2011).

211. Akhil Reed Amar, *The Fourth Amendment, Boston, and the Writs of Assistance*, 30 SUFFOLK U. L. REV. 53 (1996).

212. *Id.*

213. Entick v. Carrington, (1765) 95 Eng. Rep. 807 (K.B.).

214. *Annotation 1—Fourth Amendment*, FINDLAW, http://constitution.findlaw.com/amendment4/annotation01.html (last visited Mar. 9, 2016).

215. U.S. CONST. amend. IV.

216. *Id.*

description.[217]

The connection of the Warrant Clause to the Reasonableness Clause has caused much debate in academia as well as in the Supreme Court.[218] The underlying principle of the Fourth Amendment is a balance of the need for efficient and effective law enforcement versus the individual's right to be free from governmental intrusion.[219] It is possible to read the two clauses separately—one as regulating the reasonableness of searches and seizures, and the other as regulating the requirements for issuing valid warrants. Therefore, it imposes increased protection against the intrusion by requiring a reasonableness requirement for the intrusion in addition to the requirements imposed on the issuance of a warrant.

Although courts sometimes express a "preference" for warrants and speak of "exceptions" to the warrant requirement as both traditional[220] and modern,[221] current practice is that the exceptions often overwhelm the preference. The situations where "exceptions" apply are in fact situations when the interest underlying the Fourth Amendment are implicated to a lesser extent, such as a reduced expectation of privacy in automobiles,[222] or not implicated at all, such as items left in plain view.[223] Another justification for warrantless searches and seizures is the impracticality of obtaining a warrant in situations where there is an immediate need to preserve evidence or apprehend criminals.[224] We do not expect a law enforcement officer to stop to obtain a warrant while chasing a person who has just committed a murder into his or her house.

The Reasonableness Clause protects the individual's possessory and privacy interests. "The touchstone of the Fourth Amendment is reasonableness . . . ."[225] In 1968, the Supreme Court decided *Terry v. Ohio*.[226] In a tremendous leap, the Court recognized that when there is a reduced intrusion on the liberty of the individual, warrantless searches and seizures can be effectuated upon reasonable suspicion of the law enforcement officer that a

217. *Id.*

218. *Compare* Marron v. United States, 275 U.S. 192 (1927), *with* Go-Bart Importing Co. v. United States, 282 U.S. 344 (1931), *and* United States v. Lefkowitz, 285 U.S. 452 (1932).

219. Silverman v. United States, 365 U.S. 505, 512 (1961).

220. United States v. Robinson, 414 U.S. 218, 224–35 (1973) (holding that searches of a person incident to a lawful arrest are an exception to the warrant requirement).

221. California v. Acevedo, 500 U.S. 565, 569–70 (1991) (applying an exception to automobile searches).

222. *Id.*

223. Washington v. Chrisman, 455 U.S. 1, 5 (1982).

224. With the technological improvements, it is now possible in many states to obtain warrants through electronic communications. *See* Missouri v. McNeely, 133 S. Ct. 1552, 1562 n.4 (2013) (holding that the dissipation of alcohol was not enough to waive the requirement for a warrant for a blood test in a drunk driving case); 2 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 4.3(c), at 648–54, & 648 n.29 (5th ed. 2012) (describing oral search warrants and collecting state laws).

225. United States v. Knights, 534 U.S. 112, 118 (2001); *see also* Illinois v. McArthur, 531 U.S. 326, 330 (2001) (holding that the "central requirement" of the Fourth Amendment "is one of reasonableness" (internal quotation marks and citation omitted)); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652 (1995) (holding that "[a]s the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is 'reasonableness.'").

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

crime has occurred, or is about to occur.[227] In its decision to allow limited—both in duration and scope—stops and frisks, the Court placed "reasonableness" at the heart of the Fourth Amendment.[228] In *Terry*, the Court recognized that a brief detention is justified because the level of intrusion on the individual's interest in personal liberty is outweighed by society's interest in the investigation of criminal activity.[229] Similarly, a pat-down search for weapons is justified because the safety of a law enforcement officer outweighs the individual's interest in privacy when the law enforcement officer has reasonable suspicion to believe the individual is armed.[230] Further, due to lower intrusion on personal liberty and privacy, the court set the level of suspicion required to initiate a *Terry* stop at reasonable suspicion, a degree lower than probable cause.[231]

The Warrant Clause, on the other hand, protects the individual by requiring a neutral judicial officer to review the information available to the law enforcement officer and determine whether probable cause exists for the search or seizure.[232]

The Warrant Clause is a particularly good proxy of what is reasonable, and the courts have recognized it as such.[233] In the situations where a warrant is not required, if there is probable cause to believe a crime has occurred or about to occur, the subsequent search or seizure is reasonable.[234] The Framers believed that a warrant particularly describing the place to be searched, or the item or person to be seized, issued upon a finding of probable cause was a good balance between law enforcement interests and personal liberty.[235] Although the probable cause standard is not difficult to meet, individuals' interest in privacy of information is balanced against the needs of law enforcement.[236]

This loose connection between the Warrant Clause and the Reasonableness Clause could also mean that some searches or seizures conducted with a warrant could still be unreasonable.[237] Especially when the amount of information gained through a search is increased further than traditionally gained through a search of a house, the probable cause standard

227. *Id.*

228. "For 'what the Constitution forbids is not all searches and seizures, but unreasonable searches and seizures.'" *Id.* at 9 (citing Elkins v. United States, 364 U.S. 206, 222 (1960)).

229. *Id.*

230. *Id.*

231. *Id*

232. George R. Nock, *The Point of the Fourth Amendment and the Myth of Magisterial Discretion*, 23 CONN. L. REV. 1, 22 (1990).

233. *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 782 (1994) (noting that courts generally attached reasonableness analysis for warrantless searches and seizures); *see also* Almeida-Sanchez v. U.S., 413 U.S. 266, 269–72 (1973) (citing examples of courts rationalizing and citing reasonableness of searches in their cases).

234. Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 298–300 (1967).

235. *See* Fabio Arcila, Jr., *The Death of Suspicion*, 51 WM. & MARY L. REV. 1275, 1275 (2010) (noting that the Fourth Amendment was a means of limiting governmental search power).

236. *See Warden*, 387 U.S. at 304 (recognizing that the Fourth Amendment exists to protect one's privacy against governmental interests).

237. *Id.* at 303 ("[T]here are items of evidential value whose very nature precludes them from being the object of a reasonable search and seizure.").

may be insufficient protection under the Reasonableness Clause of the Fourth Amendment. The Supreme Court alluded to the substantial privacy interests of data stored in cell phones in *Riley v. California*.[238] While denying law enforcement officers' search of cell phones incident to arrest, the Court recognized that a warrant was available for law enforcement officers to conduct the search of the cell phone.[239] Yet, it also recognized that the amount of information, both quantitatively and qualitatively, distinguished the search of a cell phone from the search of a house:

> "[A] cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is."[240]

This stake in an individual's privacy interest is further complicated in mass collection of information, which would enable the government to track the life of a person, not only by what the person himself has done on his phone, but much more extensively with what others collected about him.[241] Until the recent advancements in technological information, it was not only impractical, but also impossible to collect the information from so many sources at the same time and store the information until such time the information is needed.[242] As further discussed below, the privacy interest at stake may leave a warrant issued upon probable cause unreasonable.

B. Property v. Privacy

Fourth Amendment protections were initially constructed on top of property rights.[243] The Court in *Boyd v. United States*[244] initially recognized that foundation in its adaptation of *Entick v. Carrington*,[245] "one of the landmark [judgments] of English liberty."[246] The *Entick* court stated that "every invasion of private property, be it ever so minute, is a trespass."[247]

The property-based protection of the Fourth Amendment was reinforced in *Olmstead v. United States*.[248] In *Olmstead*, the Court considered whether wiretapping the defendants' phones for many months constituted a search or seizure within the meaning of the Fourth Amendment.[249] The Court noted that "[s]mall wires were inserted along the ordinary telephone wires from the

238. Riley v. California, 134 S. Ct. 2473, 2493 (2014).
239. *Id.* ("Warrant is generally required before such a search.").
240. *Id.*
241. *Id.*
242. *Id.* at 2489.
243. Adams v. New York, 192 U.S. 585, 598 (1904); Boyd v. United States, 116 U.S. 616, 627 (1886).
244. *Boyd*, 116 U.S. at 627.
245. Entick v Carrington, (1765) 95 Eng. Rep. 807 (K.B.).
246. *Boyd*, 116 U.S. at 626.
247. *Id.* at 627.
248. Olmstead v. United States, 277 U.S. 438, 466 (1928).
249. *Id.*

residences of four of the petitioners and those leading from the chief office" and "[t]he insertions were made without trespass upon any property of the defendants."[250] The lack of "an official search and seizure of [defendant's] person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure" condemned the defendants.[251]

This property approach was mostly abandoned when the Court decided *Katz v. United States* in 1967.[252] In *Katz*, the issue before the Court was whether listening to a telephone conversation by attaching "an electronic listening and recording device to the outside of the public telephone booth from which [the defendant] had placed his calls" was a violation of the Fourth Amendment.[253] The Court has recognized that the "Fourth Amendment protects people, not places."[254] Further, the Fourth Amendment protects "what [a person] seeks to preserve as private."[255] The rule created by the majority was captured in a two-prong test by Justice Harlan in his concurrence.[256] Justice Harlan concluded that a search and seizure occurs when a person displays a subjective expectation of privacy, and when society accepts such expectation as reasonable. This test carries a first subjective and a second objective element.

More recently the Court revived the trespass doctrine in *United States v. Jones*.[257] The issue in *Jones* was whether GPS tracking of an individual over a long period of time was a violation of the Fourth Amendment.[258] The majority of the Court avoided the bigger question, whether constant GPS monitoring of individuals over extended periods of time is reasonable.[259] Justice Alito, writing for himself and three others would have instead applied the *Katz* test to find that constant GPS monitoring over extended periods of time is an invasion of the individual's privacy interest.[260] Justice Sotomayor, writing for herself, joined the majority in concluding that the *Katz* test supplements and does not replace the traditional trespass doctrine.[261] Yet, she went on to apply the *Katz* test.[262]

Unlike Justice Alito, Justice Sotomayor would have found that even short-term GPS monitoring is unreasonable in the absence of a search warrant, as it tends to show the most intimate details of a person's life, and therefore it is a violation of the individual's privacy interest.[263]

250. *Id.* at 456–57.
251. *Id.* at 466.
252. Katz v. United States, 389 U.S. 347 (1967).
253. *Id.* at 348.
254. *Id.* at 351.
255. *Id.*
256. *Id.* at 360–61 (Harlan, J., concurring).
257. United States v. Jones, 132 S. Ct. 945, 949 (2012).
258. *Id.* at 948–49.
259. *Id.* at 953–54.
260. *Id.* at 963–64 (Alito, J., concurring).
261. *Id.* at 955 (Sotomayor, J., concurring).
262. *Id.*
263. *Id.*

What is particularly interesting about the two concurring opinions is their focus on the information obtained from the GPS tracking.[264] The comparison of what law enforcement agencies could accomplish through the use of many officers, vehicles, and man-hours to the capabilities of technology is a weak proxy. Traditionally, the protection from long-term surveillance was practical.[265] "Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in [*Jones*]—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance."[266]

The protection offered by the Fourth Amendment is centered on the privacy interest of the individual.[267] Therefore, evaluating the privacy interest at issue in any particular case should be based on the information learned through surveillance rather than whether it could be obtained through traditional means.

C. Search v. Seizure

The majority in *Katz* did not distinguish the applicability of the test between searches and seizures.[268] Yet, the plain meaning of two words distinguishes a search from a seizure. A seizure of a person occurs "when the officer, by means of physical force or show of authority, has in some way restrained the liberty of a citizen."[269] Similarly, a seizure of property occurs when there is "some meaningful interference with an individual's possessory interests in that property."[270]

The literal meaning of a search is best described by the Court in *Lopez v. United States*:

> In every-day talk, as of 1789 or now, a man 'searches' when he

264. *Id.* at 956 (Sotomayor, J., concurring) ("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."); *id.* at 963 (Alito, J., concurring) ("Recent years have seen the emergence of many new devices that permit the monitoring of a person's movements. In some locales, closed-circuit television video monitoring is becoming ubiquitous. On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of that convenience."); *see also, e.g.*, *People v. Weaver*, 909 N.E.2d 1195, 1199–1200, (N.Y. 2009) (noting that data collected from one's GPS may disclose information private in nature).

265. *Jones*, 132 S. Ct. at 963 (Alito, J., concurring).

266. *Id.*

267. *Id.* at 954 (Sotomayor, J., concurring).

268. *Compare* Katz v. United States, 389 U.S. 353 (1967) ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment.") *with Jones*, 132 S. Ct. at 361 (Harlan, J., concurring) ("[T]he invasion of a constitutionally protected area by federal authorities is, as the Court has long held, presumptively unreasonable in the absence of a *search* warrant."). However, not much can be read into his choice of "search warrant" as search warrants commonly authorize seizure of property that is evidence of a crime. *See, e.g.*, WIS. STAT. § 968.13 (2014) (showing that search warrants are generally related to seizure of items that may constitute evidence of a crime).

269. Terry v. Ohio, 392 U.S. 1, 19 n.16 (1968).

270. United States v. Jacobsen, 466 U.S. 109, 113 (1984); *see also* LAFAVE, *supra* note 204, § 2.1(a) (5th ed. 2012) (noting that the court does not have difficulty defining what constitutes a seizure).

> looks or listens. Thus we find references in the Bible to 'searching' the Scriptures (John V, 39); in literature to a man 'searching' his heart or conscience; in the law books to 'searching' a public record. None of these acts requires a manual rummaging for concealed objects. . . . Just as looking around a room is searching, listening to the sounds in a room is searching. Seeing and hearing are both reactions of a human being to the physical environment around him—to light waves in one instance, to sound waves in the other. And, accordingly, using a mechanical aid to either seeing or hearing is also a form of searching. The camera and the dictaphone both do the work of the end-organs of an individual human searcher—more accurately.[271]

In the abstract, communication, whether through the Internet or over the phone, is difficult to fit within the categories of search or seizure.[272] Yet, technological realities, when analogized to traditional definitions, sheds light on how to categorize the access to information. As explained above,[273] most information is obtained without a physical intrusion.[274]

The literal meaning of a search, "to carefully look for someone or something[;] to try to find someone or something,"[275] is well established. Until recently there was no need to distinguish between collection and access of information because in many instances, the collection of data by the agency (for example wiretapping) and access to that information (listening to the wiretapped conversation) was simultaneous. Further, the scope of data collected and analyzed by government agencies was beyond the technological capabilities of human development.

D. Government's Subjective Intent

The Court has generally treated subjective intent of the law enforcement officer as irrelevant to the Fourth Amendment analysis. The Court never held "that an officer's motive invalidates objectively justifiable behavior under the Fourth Amendment; but [the Court] ha[s] repeatedly held and asserted the contrary."[276] Inventory searches[277] and administrative inspections[278] are the

---

271. Lopez v. United States, 373 U.S. 427, 459 (1963) (Brennan, J., dissenting) (quoting *United States v. On Lee*, 193 F.2d 306, 313 (2d. Cir. 1951) (Frank, J., dissenting)); *see also* LAFAVE, *supra* note 204, § 2.1(a) (5th ed. 2012) (defining search under the traditional approach).

272. *See* CLIFFORD S. FISHMAN & ANNA T. MCKENNA, WIRETAPPING AND EAVESDROPPING § 1:5 (2015) (noting fundamental difficulty in distinguishing between a search for a conversation and a seizure of said conversation).

273. *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).

274. *Id.*

275. *See* MERRIAM-WEBSTER ONLINE DICTIONARY (2015), http://www.merriam-webster.com/dictionary/search (last visited Mar. 9, 2016) (providing the definition of "search").

276. Whren v. United States, 517 U.S. 806, 812 (1996).

277. An inventory search is the search of property lawfully seized and detained in order to ensure that it is harmless, to secure valuable items (such as might be kept in a towed car), and to protect against false claims of loss or damage. *See* South Dakota v. Opperman, 428 U.S. 364, 369 (1976) (discussing further how different jurisdictions handle inventory searches).

278. An administrative inspection is the inspection of business premises conducted by authorities

exceptions to this general rule. When government officials conduct inventory searches or administrative inspections as a pretext to discovering incriminating evidence without probable cause, they violate the Fourth Amendment.[279]

Yet, the subjective intent of government officials may sometimes be relevant to the objectiveness analysis. In *Florida v. Jardines*,[280] the Court considered a case where police officers approached the front door of a house—an area also considered curtilage[281]—without a warrant with a drug-sniffing dog to investigate an unverified tip[282] that marijuana was being grown in the house.[283] The Court decided the case based on the property-based protection of the Fourth Amendment.[284] The Court first recognized that there was an "implied license" for the public to come into the curtilage to knock on the door.[285] Yet, "[t]he scope of [this] license—express or implied—is limited not only to a particular area but also to a specific purpose."[286] The Court held that introducing "a trained police dog to explore the area around the home in hopes of discovering incriminating evidence" was not within that implied license to enter the curtilage.[287] Consequently, the officers were trespassing into an area protected by the Fourth Amendment when they entered into the curtilage for the purpose of obtaining incriminating evidence.[288] Therefore, this act of trespass was a search within the meaning of the Fourth Amendment.[289]

The violation in *Florida v. Jardines* did not occur by the simple act of entering the curtilage; the violation occurred because police officers entered the curtilage "to engage in conduct not explicitly or implicitly permitted by the homeowner."[290] The Court stated: "no one is impliedly invited to enter the protected premises of the home in order to do nothing but conduct a search."[291] Although this language seems to inject the subjective purpose of the government official engaging in a particular conduct into the Fourth

responsible for enforcing a pervasive regulatory scheme—for example, unannounced inspection of a mine for compliance with health and safety standards. *See* Donovan v. Dewey, 452 U.S. 594, 599–605 (1981) (discussing how different jurisdictions have handled administrative inspections).

279. *See Opperman*, 428 U.S. at 379 (discussing pretextual inventory searches).

280. Florida v. Jardines, 133 S. Ct. 1409, 1416 (2013).

281. Curtilage is defined as the area "immediately surrounding and associated with the home," which is considered as "part of the home itself for Fourth Amendment purposes." Oliver v. United States, 466 U.S. 170, 176 (1984). Further, this area around the home is "intimately linked to the home, both physically and psychologically," and is where "privacy expectations are most heightened." California v. Ciraolo, 476 U.S. 207, 213 (1986).

282. An "unverified tip" is usually not enough for a finding of probable cause. Adams v. Williams, 407 U.S. 143, 147 (1972) ("Some tips, completely lacking in indicia of reliability, would either warrant no police response or require further investigation before a forcible stop of a suspect would be authorized.").

283. *Jardines*, 133 S. Ct. at 1413.

284. "[T]hough *Katz* may add to the baseline, it does not subtract anything from the Amendment's protections 'when the Government does engage in [a] physical intrusion of a constitutionally protected area.'" *Id.* at 1414 (citing United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring in the judgment)).

285. *Id.*

286. *Id.* at 1416.

287. *Id.*

288. *Id.*

289. *Id.*

290. *Id.* at 1414.

291. *Id.* at 1416 n.4.

Amendment analysis, it is likely to be limited to the context of property-based (trespass) Fourth Amendment analyses.

Further, the lack of a purpose analysis in determining whether a violation has occurred exists in other contexts as well. In *Smith v. Maryland*,[292] the Court concluded that "because individuals have no actual or legitimate expectation of privacy in information they voluntarily relinquish to telephone companies, the use of pen registers by government agents is immune from Fourth Amendment scrutiny."[293] The Court did not distinguish between the purposes of revealing information to the telephone companies. According to Justice Marshall, though, writing for the dissent, "[p]rivacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[294]

The irrelevancy of subjective intent is important because data collection and analysis is a tremendously powerful tool in law enforcement. Although local law enforcement agencies do not yet have the technical capabilities to intercept entire sets of data communications, the improvement in technology already allows them to process high amounts of data in a fraction of a second.[295] Royal Canadian Mounted Police ("RCMP") uses automatic license plate recognition technology to monitor vehicles on the road for unregistered vehicles and other criminal associations.[296] The statistics published on the RCMP's website reveal that in two years over three million license plates have been scanned, and over sixty thousand license plates have been flagged for one reason or another.[297]

E. Expectation of Privacy

Following the Supreme Court's landmark decision in *Katz v. United States*, a "search" has been understood to mean an activity that intrudes upon a citizen's "constitutionally protected reasonable expectation of privacy."[298] As articulated in Justice Harlan's concurrence, a person must exhibit a subjective expectation of privacy, and that expectation must be reasonable in the public's eye.[299]

Later courts have somewhat dialed back on the role of subjective

---

292. Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting).

293. *Id.*

294. *Id.*

295. *See, e.g.*, Tres Watkins, *Data Mining the Criminal Mind: Big Data and Law Enforcement*, SYNCFUSION (Aug. 15, 2014), https://www.syncfusion.com/blogs/post/Data-Mining-the-Criminal-Mind-Big-Data-and-Law-Enforcement.aspx (discussing various types of technologies available to law enforcement).

296. *Automatic License Plate Recognition Technology*, ROYAL CANADIAN MOUNTED POLICE, http://traffic.rcmp-grc.gc.ca/ViewPage.action?siteNodeId=23&languageId=1&contentId=11953 (last visited Mar. 6, 2016) ("The [Automatic License Plate Recognition] System is a license plate recognition program that allows vehicles observed by cameras to have their license plate read and recorded using pattern recognition software.").

297. *Id.*

298. Katz v. United States, 389 U.S. 347, 360 (Harlan, J., concurring).

299. *Id.*; LAFAVE, *supra* note 204, § 2.1 (c)

expectation of privacy as a requirement for Fourth Amendment protection.[300] It is very easy to destroy a person's subjective expectation of privacy from a position of power. This is most evident in airports where the expectation of privacy is none because of many postings around the airport telling people that they don't have an expectation of privacy.[301]

People's online presence and the tendency to share information regarding their daily lives can also be an indication of a reduced subjective expectation of privacy. Many websites inform users that they collect and analyze usage data or other information regarding the user.[302] Even the collection of the data by the government of this data raises eyebrows.[303] In this respect, the problem is how to answer the question "expectation of privacy in what?"[304] The answer is quite simply "information"—information regarding our activities, thoughts, associations, or "what hour each night the lady of the house takes her daily sauna and bath."[305]

In *Kyllo v. United States*, the Court, in considering the Fourth Amendment implications of thermal imagers, drew a bright line rule that thermal imagers, which had the capabilities to reveal intimate details of the home, could not be used to conduct a search without a warrant.[306] The Court rejected the government's argument that the thermal imager in this instance did not "detect private activities occurring in private areas," and stated that "[t]he Fourth Amendment's protection of the home has never been tied to the measurement of the quality or quantity of information obtained."[307] What the Court was concerned with was the potential of the thermal imager to obtain such information.[308]

In this respect, two proxies regarding expectation of privacy are relevant to our issue: knowing exposure to the public[309] and devices in general public use.[310]

---

300. LAFAVE, *supra* note 204, § 2.1 (c).

301. Julie Solomon, *Does the TSA Have Stage Fright? Then Why Are They Picturing You Naked?*, 73 J. AIR L. & COM. 643, 645–46 (2008).

302. *See, e.g.*, *Data Policy*, FACEBOOK, https://www.facebook.com/about/privacy (last visited Mar. 9, 2016) (describing Facebook's utilization of user data); *Welcome to the Google Privacy Policy*, GOOGLE, https://www.google.com/intl/en/policies/privacy/ (last visited Mar. 9, 2016) (describing Google's utilization of user data); *Yahoo Privacy Center*, YAHOO!, https://policies.yahoo.com/us/en/yahoo/privacy/index.htm (last visited Mar. 9, 2016) (describing Yahoo's utilization of user data).

303. Mike Gentithes, *When the Government Mines "Big Data," Does It Conduct a Fourth Amendment Search?*, CBA RECORD, Jan. 2015, at 36, 38 ("While minor government harassment that disturbs a single citizen's tranquility may be trivial and fail to reach the level of a Fourth Amendment search, it is still a greater-than-zero intrusion upon our collective tranquility interest that, when accumulated in a program as broad as the NSA's, may be sufficient to constitute a search and trigger the Fourth Amendment's protections.").

304. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012); *see also* LAFAVE, *supra* note 204, § 2.7(e) ("Perhaps the best that can be done in this brief treatment of the subject is to identify more clearly what legitimate privacy concerns attend the investigative processes here under discussion.").

305. Kyllo v. United States, 533 U.S. 27, 38 (2001).

306. *Id.*

307. *Id.*

308. *Id.*

309. California v. Ciraolo, 476 U.S. 207, 213 (1986).

310. *Kyllo*, 533 U.S. at 29.

1. Knowing Exposure to the Public

"What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[311] The idea behind knowing exposure to the public is the expectation of privacy.[312] There is no expectation of privacy on what a person reveals to the public.[313] This may explain treating light differently based on its wavelength. Visible light only passes through windows and the police can see through it. So, if the person does not have drapes, whatever is visible inside has no Fourth Amendment implications. With regard to thermal imaging, however, the infrared light emitted from the heat sources inside the house—such as people, hot showers, and heat lamps—are exposed without intention.[314]

The trouble with this standard is twofold. First, this destroys any Fourth Amendment protection to digital data. In *Smith v. Maryland*, the Court held that a person does not have an expectation of privacy in information disclosed voluntarily to a third party, such as the telephone company, including the numbers dialed.[315] Similarly, most browsing data and other information transferred on a computer travels through data centers and is in many ways exposed to a third party.[316]

The second trouble is the mental state of knowing.[317] This should be taken more strictly and more akin to intentional because even though we know everything that has heat in it will emanate in the form of infrared light, it is not necessarily true that we intend to expose the heat from the shower to others.[318]

Concerning online presence, it is simply too difficult to expect any kind of right to privacy. However, the question is not whether we display an expectation of privacy in each individual piece of information we enter on the Internet, but whether an expectation of privacy exists in all of our activities and preferences. The information gained from one's browsing history is simply far more useful and more potent than a search of the home.

In the online context, it is possible to create a very secure connection with an online server using a HTTPS protocol, which uses a two-layer communication protocol that encrypts data during transfer.[319] Yet, most websites do not offer HTTPS support, and it is not possible to unilaterally set up such a connection from the user's end.[320] Regardless of the secure connection, it is still a secure connection to a third party, from whom the

311. Katz v. United States, 389 U.S. 347, 351 (1967).

312. *Id.* at 361 (Harlan, J., concurring).

313. *Id.*

314. *Kyllo*, 533 U.S. at 27, 35.

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

316. Rus Shuler, *How Does the Internet Work?*, STANFORD (2002), https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm.

317. Katz v. United States, 389 U.S. 347, 351 (1967).

318. *See Kyllo*, 533 U.S. at 33 (discussing the importance of a subjective expectation of privacy).

319. *What is HTTPS?*, INSTANT SSL BY COMODO, https://www.instantssl.com/ssl-certificate-products/https.html (last visited Mar. 9, 2016).

320. Scott Gilbertson, *HTTPS Is More Secure, So Why Isn't the Web Using It?*, ARS TECHNICA (Mar. 20, 2011, 6:00 PM), http://arstechnica.com/business/2011/03/https-is-more-secure-so-why-isnt-the-web-using-it/.

government can obtain the information without running afoul of the Fourth Amendment.[321]

Finally, what is it that is "knowingly exposed to the public?"[322] Is it a particular piece of fact, or is it the information that several particular pieces of fact can tell about that person? With online data, each piece of information, a data point, may not be meaningful in any sense, but in aggregation as a data set, it does become meaningful and a meaning that the person never intended to reveal or never knew could be revealed.[323]

2. Devices in General Public Use

The Supreme Court developed "devices in general public use" as another proxy to determine the reasonable expectation of privacy in *Kyllo v. United States*.[324] In *Kyllo*, the police officers "suspect[ed] that marijuana was being grown in the home belonging to petitioner" and used a thermal imager to scan the home.[325] Thermal imaging devices detect infrared light in the electromagnetic spectrum.[326] The light visible to the human eye has wavelengths between 390 nanometers and 700 nanometers.[327] Infrared light has a wavelength greater than 700 nanometers and less than one millimeter (one million nanometers).[328] Therefore, infrared light cannot be seen by the naked eye without help.[329] The Court held that, when "the technology in question is not in general public use . . . obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area, constitutes a search."[330] The Court used the "general public use" as a proxy for the expectation of privacy.[331]

As highlighted by the dissent in *Kyllo*, "the contours of [the Court's] new rule are uncertain because its protection apparently dissipates as soon as the relevant technology is 'in general public use.'"[332] The earliest patent on the method for creating thermal imagers was filed as early as 1946.[333] Yet, the

321. Jennifer Valentino-Devries, *How Technology Is Testing the Fourth Amendment*, DIGITS (Sept. 21, 2011, 10:32 PM), http://blogs.wsj.com/digits/2011/09/21/how-technology-is-testing-the-fourth-amendment/.

322. *Katz*, 389 U.S. at 351 (1967).

323. Laura Lenhart, *Personal Information, Personal Property*, ILL. DIGITAL ENV'T FOR ACCESS TO LEARNING & SCHOLARSHIP, https://www.ideals.illinois.edu/bitstream/handle/2142/42118/454e.pdf (last visited Mar. 6, 2016).

324. Kyllo v. U.S., 533 U.S. 27 (2001).

325. *Id.* at 34.

326. *How Thermal Imaging Works*, INFO.COM, http://topics.info.com/How-Thermal-Imaging-Works_1502 (last visited Mar. 9, 2016).

327. Christopher Crockett, *What Is the Electromagnetic Spectrum?*, EARTHSKY (May 19, 2014), http://earthsky.org/space/what-is-the-electromagnetic-spectrum.

328. Jim Lucas, *What Is Infrared?*, LIVE SCI. (Mar. 26, 2015, 2:52 AM) http://www.livescience.com/50260-infrared-radiation.html.

329. *Id.*

330. *Kyllo*, 533 U.S. at 3 (quoting Silverman v. U.S., 365 U.S. 505, 512 (1961))

331. *Id.* ("This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.").

332. *Id.* at 47 (Stevens, J., dissenting).

333. U.S. Patent No. 2,403,066 (filed Dec. 28, 1943).

first thermal imagers were introduced in 1960s.[334] Until the 1990s, however, the cost of producing thermal imagers outweighed the benefit.[335] When the court decided the case in 2001, the cost of thermal imagers were still relatively high.[336] Now, fifteen years after the *Kyllo* decision, a thermal imager for an iPhone can be purchased for $250.[337] Thermal imagers are also used frequently by homeowners to detect parts of the house that leak heat and are in need of insulation.[338]

F. Wiretapping

Wiretapping is a highly regulated area. The Federal Wiretap Act makes it a criminal offense to intercept communications traveling on interstate or foreign commerce.[339] In *Berger v. State of New York*, the Court held "'conversation' [is] within the Fourth Amendment's protections, and that the use of electronic devices to capture it [is] a 'search' within the meaning of the Amendment . . . ."[340] Mass data collection by the National Security Agency ("NSA") reported by the news[341] and acknowledged by the Obama administration[342] has drawn much interest by the public[343] as well as academics.[344]

G. Mosaic Theory

Recent literature has focused on the idea of a "mosaic theory" of the Fourth Amendment.[345] The D.C. Circuit in *United States v. Maynard* introduced the mosaic theory.[346]

"Under the mosaic theory, searches can be analyzed as a

334. *History of Thermal Imaging*, BULLARD, www.bullard.com/V3/products/thermal_imaging/history_of_thermal_imaging.php (last visited Mar. 9, 2016).

335. FLIR, THE THERMAL REVOLUTION (June 2007), http://www.flir.com/uploadedFiles/CVS_Americas/Security/Applications/App_Notes_Revolution_a.pdf.

336. *Id.*

337. *Buy FLIR ONE*, FLIR, http://www.flir.com/flirone/display/?id=69324 (last visited Mar. 9, 2016).

338. *Thermal Imaging Cameras Explained*, GRAINGER, https://www.grainger.com/content/qt-thermal-imaging-applications-uses-features-345 (last updated Sept. 2015).

339. 18 U.S.C. § 2511 (2012).

340. 388 U.S. 41, 51 (1967).

341. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 6:05 AM), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

342. Roberts & Ackerman, *supra* note 17.

343. Susan Page, *Poll: Most Americans Now Oppose the NSA Program*, USA TODAY (Jan. 20, 2014, 3:10 PM), http://www.usatoday.com/story/news/politics/2014/01/20/poll-nsa-surveillance/4638551/.

344. *See, e.g.*, Blake Covington Norvell, *The Constitution and the NSA Warrantless Wiretapping Program: A Fourth Amendment Violation?*, 11 YALE J. L. & TECH. 228 (2009) (discussing the constitutionality of the NSA's wiretapping program).

345. David C. Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C.J.L. & TECH. 381 (2013); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012); Priscilla J. Smith, *Much Ado About Mosaics: How Original Principles Apply to Evolving Technology in* United States v. Jones, 14 N.C.J.L. & TECH. 557 (2013).

346. 615 F.3d 544, 562 (D.C. Cir. 2015).

> collective sequence of steps rather than as individual steps."[347] Identifying Fourth Amendment searches requires analyzing police actions over time as a collective "mosaic" of surveillance; the mosaic can count as a collective Fourth Amendment search even though the individual steps taken in isolation do not."[348]

The Supreme Court took the appeal from *United States v. Maynard* and analyzed the case under the Fourth Amendment.[349] The Court was divided in *United States v. Jones*.[350] Justice Scalia, writing for the Court, decided the case under the trespass doctrine.[351] Justice Alito, joined by three other justices, would have decided the case under the reasonable expectation of privacy analysis.[352] According to Justice Alito, "[s]hort-term monitoring of a person's movements on public streets accords with expectations of privacy" but "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[353] As the *Maynard* court explained:

> Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. 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.[354]

Justice Sotomayor, alone in her concurring opinion, joined Justice Scalia's opinion with regard to the application of the trespass doctrine.[355] Yet, she went further than Justice Alito's opinion with regard to the reasonable expectation of privacy analysis and explained that even short-term GPS monitoring would violate the Fourth Amendment under a reasonable expectation of privacy analysis.[356]

In order to give more context to the mosaic theory, it might be beneficial

347. *Id.*
348. Kerr, *supra* note 345, at 313.
349. United States v. Jones, 132 S. Ct. 945 (2012).
350. *Id.* at 952.
351. *Id.* at 948.
352. *Id.* at 957–64.
353. *Id.* at 964.
354. United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010).
355. *Jones*, 132 S. Ct. at 954–57.
356. *Id.* at 955.

to look at the factual scenario that occurred in *United States v. Jones*. In *Jones*, law enforcement officers installed a GPS device under the defendant's car to monitor his movements in public roads over four weeks.[357] At any individual point in time, because the defendant "knowingly exposes [his location] to the public,"[358] no search occurs. However, when an individual's movements on public roads are monitored for four weeks, the mosaic theory would hold that a search occurs because of the collective actions by the law enforcement officers.[359]

Further, there remains a question of whether individual pieces of information that do not reveal any information can become protected by the Fourth Amendment by nature of its aggregation.[360]

The mosaic theory, however, mischaracterizes when a search occurs. It is very different to say that a search does not occur when a person is viewed in a public street and when a person is followed through a GPS device for a period of time. The information gained through one is very different than the information gained through the other.[361] The mosaic theory "groups conduct that is not a search and asks if the non-searches considered together cross the line to become a search."[362] This approach presupposes that a reasonable expectation of privacy can only be in the place to be searched or the item to be seized. There are three versions of mosaic theory that outline a reasonable expectation of privacy: "societal expectations about law enforcement practices," "government power," and "whether the government learned more than a stranger could have observed."[363] All of these standards suffer from ambiguity on how to determine the society's knowledge or expectations of what others might do.[364]

However, the focus of both Justices of the Supreme Court and commentators is on what information is learned.[365] What is learned from a brief encounter on the street and constant surveillance is easily distinguishable.[366] The Fourth Amendment's protection does not depend on "measurement of the quality or quantity of information obtained"[367] by the government's surveillance technique, but what that technique has the potential

357. *Id.* at 963.

358. *Maynard*, 615 F.3d at 559.

359. *Jones*, 132 S. Ct. at 964.

360. Joseph S. Fulda, *Data Mining and Privacy*, 11 ALB. L.J. SCI. & TECH. 105, 109 (2000) ("Is it possible for data that does not in itself deserve legal protection to contain implicit knowledge that does deserve legal protection?").

361. *Maynard*, 615 F.3d at 556.

362. Kerr, *supra* note 345, at 329.

363. *Id.* at 350.

364. *See id.* (discussing in further detail how standards suffer).

365. *See* Matthew B. Kugler & Lior Strahilovitz, *Surveillance Durations Doesn't Affect Privacy Expectations: An Empirical Test of the Mosaic Theory* 5 (Univ. of Chi. Law Sch., Working Paper No. 727, 2015) (discussing the Supreme Court's focus on the types of information captured via extended surveillance and academic analysis thereof).

366. *See id.* at 36 (stating the stark differences between information obtained via lengthy surveillance and that obtained via brief tracking).

367. Kyllo v. United States, 533 U.S. 27, 37 (2001).

to reveal.[368]

H. Section 215 of the USA PATRIOT Act

Section 215 of the USA PATRIOT Act was interpreted by the NSA to allow access to personally identifiable information upon "a statement of facts showing that there are reasonable grounds to believe that the tangible objects sought are relevant . . . against international terrorism . . . ."[369] The NSA has created a program to collect and store telephone metadata through private phone companies such as Verizon Wireless.[370] The NSA's program was authorized by Section 215 of the USA PATRIOT Act.[371] It also allowed the government to compel the production of "any tangible things (including books, records, papers, documents, and other items)."[372] It is regarded as one of the most expensive pieces of legislation authorizing government activity, and even the drafter of the act does not support that reading of the statute.[373]

IV. ANALYSIS

From the review of the case law and commentators it is evident that the activities of the government run afoul of the Fourth Amendment when those activities have potential to reveal information in excess of what the government could traditionally learn without warrants.[374] The highest protection of the Fourth Amendment is at home[375] because of the information contained inside the four corners of the home and blocked by the walls.[376] These intimate details are what separate the home from other places, and these intimate details are what the Fourth Amendment ought to protect.

A. Reasonable Expectation of Privacy in Life

One of the biggest difficulties in scrutinizing the collection and analysis

368. *See id.* at 38 (discussing what information is revealed by the use of a thermal imaging device and the circumscriptions on the information as contemplated by the Fourth Amendment).

369. USA PATRIOT Improvement and Reauthorization Act of 2005, 50 U.S.C. § 1861(b)(2)(B) (2012).

370. For a detailed discussion of phone metadata collection and related Supreme Court jurisprudence, see Nathaniel Wackman, *Historical Cellular Location Information and the Fourth Amendment*, 2015 U. Ill. L. Rev. 263 (2015), which provides a detailed discussion of phone metadata collection and related Supreme Court jurisprudence. For a discussion of the challenge against NSA program, see Susan Freiwald, *Nothing to Fear or Nowhere to Hide: Competing Visions of the NSA's 215 Program*, 12 COLO. TECH. L.J. 309, 323 (2014), which discusses the challenges against the NSA's surveillance programs.

371. 50 U.S.C. § 1861(c)(2)(F)(iv).

372. 50 U.S.C. § 1861(a)(1).

373. *Sensenbrenner: PATRIOT Act Needs Changes After NSA Revelations*, WISPOLITICS.COM, (June 24, 2013 9:26 AM), http://dc.wispolitics.com/2013/06/sensenbrenner-patriot-act-needs-changes.html ("[NSA activities leaked by Edward Snowden] certainly was not what was contemplated when the PATRIOT Act was passed.").

374. *See generally id.* (revealing Rep. Sensenbrenner's belief that Snowden's releasing classified information showed the public that the law was being used in ways that were unintended in the original debate).

375. Kyllo v. United States, 533 U.S. 27, 40 (2001) (citing Payton v. New York, 445 U.S. 573, 590 (1980)).

376. *Id.*

of data by the government is the knowing exposure of this information to third parties.[377] Most of the data exchanged over the Internet is necessarily shared with ISPs and at least the information that you are trying to receive is shared.[378] This particular limitation defeats the Fourth Amendment protection just because of how the Internet is set up.

The acts and communications displayed in the virtual environment through our use of technology to track our lives would suggest that people do not have that expectation of privacy. In a more traditional approach to the Fourth Amendment, our individual acts of revealing certain information to third parties, as articulated above, suggests that there is no expectation of privacy. Even then, however, no one in 1776 would have expected that when he or she shares certain information with certain people, those people would get together and share their knowledge. It would be unreasonable to expect people to do so. A person in 1776 would have a privacy interest in the aggregated information, because aggregated information is our lives.

At least one circuit court has already articulated this position in *Reeves v. Churchich*.[379] The court held that pointing a rifle at a premises occupant, even if the end of the rifle was inserted inside those premises and "constituted a common law trespass," nonetheless was "not a Fourth Amendment violation" because "the rifle was incapable of obtaining information."[380] The outcome of *Reeves* might be different in light of *Jones v. United States*, however, where the Court reviewed the technical trespass further[381] and reflected the premise that the privacy is in the information and not simply how it is obtained.[382]

Further, the courts have already considered technological devices that gather certain information and characterized the use of such devices as a search.[383] In *United States v. Epperson*, in concluding that the use of a magnetometer was a search, the court stated, "a government officer, without permission, discerned metal on Epperson's person."[384] These increased technologies do not simply "*enhance* police senses as they do *replace* them with something superhuman, an ability to perceive that people simply do not have."[385] These devices give new information to the officer—information they

377. Katz v. United States, 389 U.S. 347, 351 (1967).

378. *See* Rory Cellan-Jones, *Web Surveillance—Who's Got Your Data?*, BBC NEWS (Apr. 2, 2012), http://www.bbc.com/news/technology-17586605 (articulating the position that while ISPs may not collect personally identifiable information, they are collecting metadata on their users).

379. Reeves v. Churchich, 484 F.3d 1244 (10th Cir. 2007).

380. *Id.* at 1256.

381. *See* United States v. Jones, 132 S. Ct. 945, 951 n.5 (2012) (discussing the general principle that a trespass must be conjoined with an attempt to gain information to constitute a search).

382. *See Reeves*, 484 F.3d 1244 (illustrating that the right to privacy and protection against unlawful searches attaches to specific information sought to be kept private and not simply the means by which law enforcement might search).

383. *See* LAFAVE, *supra* note 204 (elaborating on the impact of the expansion of technology and court opinions that have limited such technology being used to conduct surveillance on American citizens).

384. United States v. Epperson, 454 F.2d 769, 770 (4th Cir. 1972).

385. David A. Harris, *Superman's X-Ray Vision and the Fourth Amendment: The New Gun Detection Technology*, 69 TEMP. L. REV. 1, 24 (1996) (emphasis added); *see also* Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, 10 HARV. J.L. & TECH. 383, 447–52 (1997) (reaching same conclusion and discussing proposed limitations on use of such devices).

could not otherwise obtain or gather.[386]

In describing "the right to be let alone" Justice Brandeis, in his dissenting opinion in *Olmstead v. United States*, stated the Framers "sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations.[387] They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[388] Although the Fourth Amendment does not give "a general constitutional 'right to privacy,'"[389] it does protect "what he [or she] seeks to preserve as private, even in an area accessible to the public."[390] What he or she seeks to preserve as private is information about himself or herself—thoughts, beliefs, and browsing history.[391] After all, "the Fourth Amendment protects people, not places."[392]

Imagine that a police officer is standing in a pitch-dark room, and there is nothing in his reaching distance.[393] Standing there in the room, the officer cannot learn anything. He can try to look for things but his capability to do so is limited by his eyes. Because there is no information gained, no search occurs.

B. Information Gathering is Not Seizure

Information gathering is not seizure because there is no "meaningful interference with an individual's possessory interests in" information.[394] First, as discussed above, "[d]ata in its ethereal, non-physical form is simply information . . . ."[395] It is difficult to conceptualize how one can seize information. It is possible to seize items containing information, such as papers or hard drives, but information itself is not seized. Second of all, although there is a privacy interest in information, it does not translate to a possessory interest.[396] Finally, there is no meaningful interference with the flow of information. Just as in *Katz*, the information continues to flow and it is copied rather than intercepted.[397]

Yet, data gathering, even without the analysis, can have a substantial

386. *See* Slobogin, *supra* note 385, at 385 (discussing some of the general applications of surveillance technology in law enforcement).

387. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

388. *Id.*

389. Katz v. United States, 389 U.S. 347, 350 (1967).

390. *Id.* at 351.

391. *See generally* Nathan Freed Wessler, *How Private Is Your Online Search History?*, AM. C.L. UNION (Nov. 12, 2013, 12:04 PM), http://www.aclu.org/blog/how-private-your-online-search-history (exploring the privacy of web browser and Internet search history).

392. *Katz*, 389 U.S. at 351.

393. For the purposes of this example assume there is no trespass.

394. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

395. Digitech Image Techs., LLC v. Elecs. for Imaging, Inc., 758 F.3d 1344, 1350 (Fed. Cir. 2014).

396. *See* Steven G. Davison, *Warrantless Investigative Seizures of Real and Tangible Personal Property by Law Enforcement Officers*, 25 AM. CRIM. L. REV. 577, 599 (1988) (highlighting the distinction between "possessory interests" and "privacy interests" in the context of searches and seizures under the Fourth Amendment).

397. As discussed above in Part II, some of the techniques do allow for interception of the data and such techniques may implicate the Fourth Amendment. This point is outside the scope of this project.

chilling effect on peoples' activities. Knowing that every act is recorded by the government, individuals might be reluctant to visit certain websites or engage in certain activities in fear of being recorded and later flagged by the government. Although over-deterrence is a risk, procedural safeguards as articulated below should reduce this chilling effect, as the access to information will be regulated by the Fourth Amendment.

C. Acquisition v. Access

There are two distinct points where a potential violation of this privacy interest in information can occur: during initial acquisition of information and during access of information.[398] Information acquisition usually occurs in increments as pieces of information gathered from various sources.[399] Information access is a more continuous endeavor. Gathered information data points are collectively displayed or analyzed for patterns and meaningful data sets.[400]

Information access fits the definition of search better than information acquisition.[401] Only during access to information does the individual or the automated program "try to find someone or something."[402] At this stage, the officer or the computer program searches individual data points and fits them into categories that reveal other information of interest.[403]

During the gathering stage, information is copied in bits and pieces.[404] As proponents of mosaic theory suggest, there is a problem with gathering individual pieces, which would amount to an unreasonable search.[405] Yet, the sequence of events that goes from individual data acquisition to the aggregated data simply does not fit into any literal meaning of search.[406] As discussed above, most acquisition methods do not distinguish between the information

398. *See generally* Mark Taticchi, *Redefining Possessory Interests: Perfect Copies of Information as Fourth Amendment Seizures*, 78 GEO. WASH. L. REV. 476, 477–78 (2010) (discussing the expected rights individuals have in their information and how access and duplication of information is problematic vis-à-vis Fourth Amendment jurisprudence).

399. *See generally* Rakesh Sharma, *Google's Acquisition of Nest and Your Privacy*, FORBES (Jan. 13, 2014, 9:07 PM), http://www.forbes.com/sites/rakeshsharma/2014/01/13/googles-acquisition-of-nest-and-your-privacy/#1df42ce3fdf5 (providing an example of incremental acquisition of personal data).

400. *Id.* ("Google can easily combine this data set with other services to gain an even more complete picture of your movements.").

401. *See* MERRIAM-WEBSTER ONLINE DICTIONARY (2015), http://www.merriam-webster.com/dictionary/search (last visited Mar. 9, 2016) (providing the definition of "search").

402. *Id.*

403. *See generally* Doug Wyllie, *How 'Big Data' Is Helping Law Enforcement*, POLICEONE.COM (Aug. 20, 2013), http://www.policeone.com/police-products/software/Data-Information-Sharing-Software/articles/6396543-How-Big-Data-is-helping-law-enforcement/ (discussing how data analytics can improve law enforcement and the role of the crime analyst in utilizing data sets).

404. *See* Christina DesMarais, *Who's Gathering Your Personal Information?*, TECHLICIOUS (Mar. 14, 2014), http://www.techlicious.com/blog/whos-gathering-your-personal-information/ (illustrating the fragmented way personal information and online data is aggregated by data collectors).

405. *See* Kugler and Strahilovitz, *supra* note 365, at 5 (illustrating Mosaic Theory proponents' concerns over the piecemeal collection of a private individual's information).

406. *See generally* Kerr, *supra* note 304, at 315–20 (articulating a historical approach to applying Fourth Amendment law to searches and seizures and its poor fit to questions and problems arising in Mosaic Theory).

until it is processed.[407] Even though it is possible to create a program to only store information that is relevant,[408] everything is gathered and analyzed, and the irrelevant data is deleted.[409]

At the most fundamental level, in order to be able to copy data stored on a computer hard drive, the computer needs to read each bit to copy.[410] However, the individual bit does not reveal anything, as it is either a one or zero.[411] Only when those zeros and ones are put together can the machine make sense of it.[412] However, during the copying stage the act of looking at each individual bit does not reveal any information; therefore no search occurs.[413]

The reason why there is no search at any individual time on the public streets—that there is no reasonable expectation of privacy in that information—is the same for the online context. There is no individual expectation of privacy in each individual piece of information. However, the reason why the aggregated data feels like a violation is not because the information is out there, it is because the information is accessed all at the same time.[414] Information sitting in computer hard drives throughout the country in the servers of various companies does not violate any privacy interests.[415] Similarly, when the government gathers data, if it is just sitting in the computer hard drives of massive data centers, no violation occurs because no information is gained.

When the information is accessed in a meaningful format, only then a violation occurs because it reveals information protected by the privacy interest.[416]

D. How Much Is Too Much

The difficulty in characterizing the reasonable expectation of privacy in information, or any other theory that depends on a mosaic theory—that

407. FELDMAN & SANGER, *supra* note 201, at 64 ("Probably the most common theme in analyzing complex data is the classification, or categorization, of elements. Described abstractly, the task is to classify a given data instance into a prespecified set of categories.").

408. Relevant information could be a keyword, particular name, a phone number, or an address.

409. *See* Charles Arthur, *What Is Google Deleting Under the 'Right to be Forgotten'—and Why?*, GUARDIAN (July 4, 2014, 12:46 PM), http://www.theguardian.com/technology/2014/jul/04/what-is-google-deleting-under-the-right-to-be-forgotten-and-why (providing an example of a large data-collecting company sorting its collected information and discarding what is irrelevant).

410. *How Coding Works*, CODECONQUEST, http://www.codeconquest.com/what-is-coding/how-does-coding-work/ (last visited Mar. 9, 2016) ("A computer can only understand two distinct types of data: on and off. In fact, a computer is really just a collection of on/off switches (transistors). Anything that a computer can do is nothing more than a unique combination of some transistors turned on and some transistors turned off.").

411. Each digit in binary code represents one transistor. *Id.* Binary code is based on ones and zeros arranged in combinations of eight. *Id.* A single one or zero is only meaningful when it is read relative to the other seven digits that comprise a byte. *Id.* ("Modern computers contain millions or even billions of transistors, which means an unimaginably large number of combinations.").

412. *Id.*

413. Chris Woodford, *Hard Drives*, EXPLAINTHATSTUFF, http://www.explainthatstuff.com/harddrive.html (last updated Aug. 24, 2015).

414. *Id.*

415. *Id.*

416. The question remains, however, whether a violation occurs when an automated computer program searches the computer or only when a government official reviews the computer's findings.

individual information obtained without violating the Fourth Amendment can nevertheless violate the Fourth Amendment in the aggregate—is made clear by the next logical question: How much data is too much? A local police department collecting traffic camera images from a single town's traffic lights and gathering travel information about the drivers is much different than the mass surveillance and collection of phone records by NSA.

The issue is when does data become "aggregated?" "[A]gencies and departments maintain almost 2000 databases, including records pertaining to immigration, bankruptcy, Social Security, military personnel, as well as countless other matters . . . . States maintain public records of arrest, births, criminal proceedings, marriages, divorces, property ownership, voter registration, workers compensation, and scores of other types of records," including licensing records "on numerous professionals such as doctors, lawyers, engineers, insurance agents, nurses, police, accountants, and teachers."[417] This information as it is held at individual agencies does not pose a problem, as the "practical obscurity"[418] still keeps the information that is revealed by the collective analysis of that individual information private.[419]

The single biggest concern that relates to the privacy concern of the aggregated data is the practical obscurity. Information revealed to third parties,[420] the tracking of movement in public streets,[421] and information shared on public websites, can all individually be obtained by various methods such as FOIA or by subpoena from various entities that store such information.[422] Only when the practical obscurity is removed does the data become aggregated.[423] Therefore, the data becomes aggregated when a system is set up for accessing that information from a single access point.[424]

This formulation of aggregation therefore allows for flexibility on government agencies' procedures for digitizing records and storing information relevant to the agencies' function, while protecting against the aggregated access to that information. This formulation does not depend on the agencies' purpose either. Even if an agency has a completely legitimate purpose, such as the IRS setting up a system to control the accuracy of individuals' tax filings, when the system acts to collect information from various sources, or allows access to that information from a single access point, the data becomes aggregated for the purposes of the Fourth Amendment.

E. Level of Suspicion

The level of suspicion to access the aggregated information should be a

417. Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1403 (2001).

418. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762 (1989).

419. *Id.*

420. Smith v. Maryland, 422 U.S. 735, 744 (1979); Klayman v. Obama, 957 F. Supp. 2d 1, 40 (2012).

421. United States v. Jones, 132 S. Ct. 945, 946 (2012).

422. *Id.*

423. *Id.*

424. Under this theory there would be a question whether a computer program that analyzes only data available on the Internet would fall under such definition of single access point.

preponderance of the evidence, a standard higher than probable cause. The intrusion into an individual's privacy interest in the aggregated data is much higher than a traditional search because the access to aggregated data reveals much more information than a traditional search of a house.[425]

"The touchstone of the Fourth Amendment is reasonableness . . . ."[426] As the Court articulated in *Terry v. Ohio*,[427] when the intrusion into one's protected interest is low, a lower standard of suspicion is sufficient to justify a search and seizure.[428] In the case of access to aggregated data, the weights are reversed. The intrusion into the privacy interest of the individual is much more significant than the brief investigatory stop. It implicates information regarding the entire life of the individual.[429] Although the national security interest is also much higher than shoplifting, the Fourth Amendment binds every law enforcement officer, from the county constable to the NSA.[430] For that end, even a probable cause standard may fall short of providing a justification for the intrusion.

The level of privacy interest in electronic data is somewhat recognized in *Riley v. California* where the Court held that a warrantless search of a cell phone incident to arrest was unreasonable.[431] Although the Court did consider that a warrant issued by a magistrate judge would be sufficient, the aggregated information is even more intrusive than the contents of the cell phone.[432] The aggregated information by its "nature precludes [it] from being the object of a reasonable search."[433] Therefore, when the search is unreasonable, even the warrant issued upon probable cause would be unreasonable.[434] Due to the nature of information gathered from a search of aggregated data, and its tendency to reveal much more information than a search of a house or work place, access to that information deserves a finding of a higher suspicion level than probable cause.

In that regards, the preponderance of evidence standard would allow a greater protection to the information while balancing the needs of law enforcement in the investigation of targeted individuals. Even though probable cause to arrest an individual or search his house will be satisfied before the access to aggregated information is allowed, the information gathered from the aggregated data will be much more than a search of the house or interrogation of the individual.[435]

---

425. *How Smart Meters Invade Individual Privacy*, SMART GRID AWARENESS, http://smartgridawareness.org/privacy-and-data-security/how-smart-meters-invade-individual-privacy/ (last visited Mar. 9, 2016).

426. United States v. Knights, 534 U.S. 112, 118 (2001) (citing Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

427. 392 U.S. 1, 9 (1968) (citing Elkins v. United States, 364 U.S. 206, 222 (1960)).

428. *Id.* at 26.

429. *See* United States v. Jones, 132 S. Ct. 945, 954 (Sotomayor, J., concurring).

430. U.S. CONST. amend. IV.

431. 134 S. Ct. 999 (2014).

432. *Id.*

433. Warden v. Hayden, 387 U.S. 294, 303 (1967).

434. *Id.*

435. *Id.*

F. Efficient Law Enforcement, Potential for Abuse

Use of technological developments increases the efficiency of law enforcement.[436] Until recent years, the amount of information law enforcement officers could gather was limited by the capabilities of the individual officers. It was about asking questions, physically following a person in the streets, and stakeouts. Most surveillance methods were procedurally inefficient.[437] The ease of obtaining information, however, should not be a case against such techniques. On the contrary, it should be a case for the use of such techniques.

Technological data analysis methods allow for more automation. Automation can be taught[438] or programmed without relation to individuals' constitutionally protected characteristics such as race, national origin, and gender. Even though a program can be tweaked to take into account such characteristics, it would be easier to show these violations than the current struggle regarding law enforcement agencies' motives in enforcing the law. Moreover, when there is a neutral reason for the disparate impact based on a characteristic, it can be shown with reference to the program.

As seen in the example of Canadian license plate readers, most violations identified by the system will go untreated because of administrative limitations.[439] Yet, automation would allow more efficient distribution of law enforcement resources. For example, the automated software could be programmed to rank or classify findings based on offense types, the distance from an on-duty police officer, or the evidentiary value that gives rise to a suspicion. This allows for objective determinations in crime investigations while leaving enough discretion to compensate for the shortcomings of the software.

"Great power comes with great responsibility,"[440] yet we still see on the television the abuse of power by the government. These abuses range from the reports of NSA employees exchanging intimate photos,[441] to everyday police officer brutalities,[442] to systematic police department cultures.[443] The primary

436. K.A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 2 (2003) ("The efficiencies inherent in data aggregation itself cannot be denied; indeed, it is these efficiencies that provide the impetus for developing and employing data aggregation technologies in the first place."); *see also* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 506–11 (2006) (explaining more on the problems of data aggregation).

437. During oral arguments in *Jones v. United States*, Chief Justice Roberts asked the government's lawyer Mr. Dreeben whether the Constitution would allow the FBI to install a GPS device on their cars.

438. Machine learning algorithms are common in data mining.

439. Douglas Quan, *'You Are Being Tracked': How Cities Use License-Plate Scanners to Create Vast Databases of Vehicle Sightings*, NAT'L POST (July 14, 2014), http://news.nationalpost.com/news/canada/you-are-being-tracked-how-cities-use-licence-plate-scanners-to-create-vast-databases-of-vehicle-sightings (last updated Jan. 24, 2016, 10:21 PM).

440. SPIDER-MAN (Marvel Entertainment 2002).

441. Steve Dent, *Snowden Shows John Oliver How the NSA Can See Your Dick Pics*, ENGADGET (Apr. 6, 2015), http://www.engadget.com/2015/04/06/john-oliver-snowden-interview/.

442. ANDREA J. RITCHIE, ESQ. ET AL., U.N. COMM. ON THE ELIMINATION OF RACIAL DISCRIMINATION, IN THE SHADOWS OF THE WAR ON TERROR: PERSISTENT POLICE BRUTALITY AND ABUSE OF PEOPLE OF COLOR IN THE UNITED STATES (Dec. 2007).

443. U.S. DEP'T OF JUSTICE, CIVIL RIGHTS DIV., INVESTIGATION OF THE FERGUSON POLICE

concern for the Fourth Amendment—the dislike of general warrants—can be implicated as the ease of accessing information stored in a data center increases and as the loss of "practical obscurity"[444] "magnifies and enhances government power"[445] and creates the temptation to abuse such power.[446]

Although these cultural systematic cultural problems are horrifying, it does not involve the Fourth Amendment analysis. The Fourth Amendment "protects individual privacy against certain kinds of governmental intrusion"[447] but not others.[448] Further, "[i]t is the exploitation of technological advances that implicates the Fourth Amendment, not their mere existence."[449] Therefore the "access" to the information rather than the gathering of the information is what implicates the Fourth Amendment.

V. RECOMMENDATION AND CONCLUSION

The speed at which information is gathered and analyzed is beyond what the people of 1776 could have imagined. This information, in the aggregate, allows for effective law enforcement and other government activities. However, the removal of practical obscurity regarding the access to information creates significant privacy concerns. The Fourth Amendment's protection against unreasonable searches and seizures is one of the constitutional safeguards against a particular governmental intrusion.[450] There is information stored in databases of various governmental agencies and private corporations that can be obtained by the government without any Fourth Amendment implications.[451] However, when a system is created to remove the practical obscurity of obtaining the aggregated information and allow access from a single access point when the data is aggregated, then the access to that aggregated information in such a manner implicates the Fourth Amendment far beyond the use of any other device.[452] Regardless of the agencies' purpose in creating such a system, when the system is capable of obtaining such information, the Fourth Amendment will be violated. Further, the probable cause standard of the Fourth Amendment is dwarfed by the tremendous privacy intrusion, and even a warrant issued upon a finding of probable cause does not satisfy the reasonableness requirement of the Fourth

---

DEPARTMENT, http://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/04/ferguson_police_department_report.pdf; *see also* Ta-Nehisi Coates, *The Gangsters of Ferguson*, ATLANTIC (Mar. 5, 2015), www.theatlantic.com/politics/archive/2015/03/The-Gangsters-Of-Ferguson/386893/ (examining results of the Department of Justice's report on the shooting of Michael Brown and investigation into the Ferguson Police Department's practices).

444. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762 (1989).

445. Taipale, *supra* note 436.

446. *Id.*

447. Katz v. United States, 389 U.S. 347, 350 (1967).

448. *See id.* at 363 n.** (stating as an example that "[t]he Fourth Amendment does not protect against unreliable (or law-abiding) associates." (citation omitted)).

449. United States v. Karo, 468 U.S. 705, 712 (1984).

450. *Katz*, 389 U.S. at 350.

451. *Id.* Under this theory there would be a question whether a computer program that analyzes only data available on the Internet would fall under such definition of single access point.

452. *Id.*

Amendment.[453] Hence, only upon a preponderance of evidence can a law enforcement agency have access to aggregated data.

As with any other area where privacy is concerned, Congress could easily regulate the access to aggregated information and create procedural safeguards that allow a degree of privacy while leveraging the technological power to detect and prevent crime. As Justice Alito suggested, the use of many data gathering and analyzing technology is not that different from traditional wiretapping, yet they are much more powerful.[454] The Fourth Amendment's protections have been highly debated and have seen a lot of changes in recent years. However, the impact of technology on Fourth Amendment jurisprudence has yet to reach its peak.

453. U.S. CONST. amend. IV.
454. United States. v. Jones, 132 S. Ct. 945, 956 (2012) (Alito, J., concurring).