The Use of Clearview AI to Support Warrants Violates the Fourth Amendment

Kevin Johnson
The Use of Clearview AI to Support Warrants Violates the Fourth Amendment

Cover Page Footnote
* J.D. Candidate, Fordham University School of Law, 2024; B.S., University of California, San Diego, 2018. I would like to thank Professor Weinstein and the editors and staff of the Fordham Intellectual Property, Media and Entertainment Law Journal for their invaluable help and insight. Lastly, I would like to thank my mom and sister.
The Use of Clearview AI to Support Warrants Violates the Fourth Amendment

Kevin Johnson*

Social media platforms encouraged millions of Americans to post hundreds of photos of themselves on the Internet. Clearview AI, a tool that harnesses “publicly available” online images for facial recognition, violated those platforms’ terms of service to collect those photos and in doing so de-anonymized millions of Americans. This Note examines the Fourth Amendment implications of law enforcement’s use of Clearview AI and its compatibility with constitutional protections. This Note argues that the use of Clearview AI by police to support warrant applications runs afoul of established legal standards by analyzing the evolution of Fourth Amendment jurisprudence in light of technological advancements.

The foundation of the argument is twofold: first, that the current jurisprudential landscape has increasingly recognized the need to adapt constitutional protections to the digital age, acknowledging the unique capabilities of digital surveillance to bypass traditional privacy safeguards; and second, that Clearview AI embodies a form of digital surveillance that is particularly invasive due to its comprehensive and indiscriminate collection of personal data. This Note delves into how Clearview AI’s capabilities trigger the very concerns the Fourth Amendment intends to protect against—preventing law-abiding citizens from being put in a perpetual police line-up without probable cause or judicial oversight.

* J.D. Candidate, Fordham University School of Law, 2024; B.S., University of California, San Diego, 2018. I would like to thank Professor Weinstein and the editors and staff of the Fordham Intellectual Property, Media and Entertainment Law Journal for their invaluable help and insight. Lastly, I would like to thank my mom and sister.
Ultimately, this Note concludes by arguing that law enforcement’s unchecked use of Clearview AI not only undermines the privacy expectations of individuals but also contravenes the principles embedded within the Fourth Amendment. This Note advocates for a reassessment of how privacy rights are enforced in the digital realm, urging a reevaluation of the boundaries of government surveillance in maintaining the constitutional balance between advancing technology and fundamental civil liberties.

INTRODUCTION ................................................................. 993

I. WHAT IS FACIAL RECOGNITION & CLEARVIEW AI? ................................................. 996
   A. Background on Facial Recognition Technology ............................................. 997
   B. Clearview AI Has Revolutionized the Field of Facial Recognition Technology .......... 998
      1. Clearview’s Claim That Their Database Only Uses “Publicly Available Images” Requires Context ............................................. 999
   C. Most Americans Are in Clearview’s Database ............................................ 1001
   D. Police Are Using Clearview Search Results to Support Warrants ......................... 1002

II. THE FOURTH AMENDMENT ADAPTS TO NEW TECHNOLOGY................................. 1004
   A. The Fourth Amendment Was Originally Only Concerned With Physical Trespass ...... 1005
   B. Twentieth Century Supreme Court Holdings Limited Fourth Amendment Protections to Physical Trespass................................. 1006
   C. The Court Has Expanded Fourth Amendment Protections to Cover More Than Physical Trespass to Protect Society’s Changed Expectation of Privacy ................................. 1007
   D. The Court has Expressed Concern when New Technology Provides Law Enforcement with a “Superpower” that Triggers Fourth Amendment
E. The Court Has Acknowledged Digital Surveillance Possesses Unique Characteristics, Making It Capable of Circumventing Traditional Human Privacy Barriers .................................................. 1013

III. CIRCUIT COURT RULINGS REVEAL THE FOURTH AMENDMENT IS NOT CONCERNED WITH DIGITAL SURVEILLANCE SYSTEMS THAT ARE TARGETED .............................................................. 1017

IV. HOW CLEARVIEW AI IMPLICATES THE FOURTH AMENDMENT .......................................................... 1021
   A. Clearview’s Legal Justification for the Warrantless Use of Their Technology Is Insufficient to Justify the Warrantless Use of Their Technology .................................................. 1021
   B. Individuals Have a Reasonable Expectation of Privacy in Photos They Post ......................... 1023
   C. Individuals Have a Reasonable Expectation of Privacy in Photos of Themselves That Are Posted by Someone Else .................................................. 1026

CONCLUSION .................................................................................................................. 1027

INTRODUCTION

Every day, around ninety-five million photos and videos are posted on Instagram;¹ some project the platform will have 1.44 billion monthly active users worldwide by 2025, which would represent 31.2% of global internet users.² Instagram, Facebook, WhatsApp, and Facebook Messenger, all of which are owned by

Meta, have a combined 3.64 billion monthly active users globally. LinkedIn has 66.8 million monthly active users in the United States, with 87% of recruiters finding LinkedIn the most effective platform for vetting job applicants. Importantly, “[t]he internet was built to facilitate the posting of public information, and social media platforms entrenched this idea; [for example,] Facebook recruited a billion users between 2009 and 2014, when posting publicly . . . was [Facebook’s] default setting.” Other sites, such as “YouTube, Twitter, and LinkedIn[,] encourage public posting as a way for users to gain influence, contribute to global conversations, and find work.”

A typical Facebook user uploads an average of 217 photos, with 66,000 photos shared to Instagram every minute. Clearview AI was the first company to extract these photos through a process called “scraping” and store them in a database.

---


5 Id.


7 Id.

8 Cooper Smith, Facebook Users Are Uploading 350 Million New Photos Each Day, BUS. INSIDER (Sept. 18, 2013, 8:00 AM), https://www.businessinsider.com/facebook-350-million-photos-each-day-2013-9 [https://perma.cc/WUX3-EDZ7] (“Facebook revealed in a white paper its users have uploaded more than 250 billion photos and are uploading 350 million new photos each day. To put that into perspective, that would mean each of Facebook’s 1.15 billion users have uploaded an average of 217 photos apiece. These numbers do not include photo uploads on Instagram.”).


10 Cloudflare, What Is Data Scraping?, CLOUDFLARE, https://www.cloudflare.com/learning/bots/what-is-data-scraping/ (last visited Mar. 26, 2024) (“Data scraping, in its most general form, refers to a technique in which a computer program extracts data (like photos) from output generated from another program. Data scraping is commonly manifest in web scraping, the process of using an application to extract valuable information from a website.”).
It scrapes not only from social media platforms, but from “the whole Internet.” Clearview AI uses revolutionary facial recognition software, trained using “publicly-available” photographs from the Internet, to create a “Google-like” search engine for faces. A Clearview AI user can upload a picture of a stranger’s face to the platform and receive URLs to almost every website where that face appears. Further, it does not matter how old the uploaded picture is; Clearview AI’s software accounts for “age progression, variations in poses and positions, changes in facial hair, and many [other] visual conditions.” In this way, Clearview AI’s platform operates like an inverse Google search, using faces to find names. Clearview AI has “turned faces into name tags.”

Currently, Clearview AI’s platform is only accessible to law enforcement, government agencies, and the military. For around

---

14 LastWeekTonight, *supra* note 11, at 12:45.
18 *Id.* at 0:50.
19 *Company Overview*, *supra* note 12.
$6,495 per year, police can identify anyone that has a picture on the Internet. Critics argue this puts millions of law-abiding citizens into a “perpetual police line-up.”

This Note will argue three things: first, case law has already articulated where the capabilities of advanced digital surveillance tools run afoul of the Fourth Amendment; second, Clearview AI has many of the capabilities that trigger Fourth Amendment concerns; and lastly, Clearview’s legal argument justifying the unchecked use of their technology is a misinterpretation of Fourth Amendment case law. Part I outlines the general background on facial recognition technology and explains how Clearview AI revolutionized the facial recognition field. Part II analyzes the evolution of Fourth Amendment case law and argues its protections have been and continue to be extended and adapted to cover new technologies. Additionally, Part II will argue that the Supreme Court has articulated the specific capabilities of digital surveillance that implicate the Fourth Amendment. Part III looks at recent circuit court holdings decided in the context of modern digital surveillance systems to further define the technological capabilities that are most pertinent to Fourth Amendment analysis. Finally, Part IV argues that Clearview AI has many of those capabilities, and thus should trigger Fourth Amendment protections.

I. WHAT IS FACIAL RECOGNITION & CLEARVIEW AI?

The Fourth Amendment protects individuals from unreasonable searches and seizures by the government. “Fourth Amendment

---


22 U.S. CONST. amend. IV.
jurisprudence is... fact-specific, with multiple competing doctrines informing the courts’ decision-making as to what new... technology [uses] constitute searches or seizures.” Section I.A explains how the “new technology” of facial recognition works. Section I.B explains why Clearview AI is vastly different and more powerful than prior facial recognition systems, and why we need Fourth Amendment protections prohibiting unchecked law enforcement usage. Section I.C will show that nearly every American is affected by Clearview AI, making this an issue of national concern. Lastly, Section I.D presents evidence that police departments are using Clearview AI contrary to its intended use.

A. Background on Facial Recognition Technology

Fundamentally, digital facial recognition technology automatically identifies an individual based on a digital image or video frame. Facial recognition technology uses an algorithm to match the face from an uploaded photo to an existing photo (or photos) in a database. The algorithm takes hundreds of measurements of the facial characteristics present in an input photo, such as the precise location of the eyes, scars, or other facial differences that define that individual’s face. It then compares the measurements taken from the input photo to a database of known faces to find a photo that matches the measurements of the input photo. If the database of known faces has names attached to the photos, the user would also learn the name of the person when the algorithm makes a match.

25 See Clearview AI Principles, supra note 16.
28 For example, say a database consisted of state driver’s license photos; when the algorithm matches the face to the individual’s driver’s license, the police would have their
B. Clearview AI Has Revolutionized the Field of Facial Recognition Technology

When a user uploads an image to Clearview’s website, its proprietary algorithm processes the image and matches it to existing photos within Clearview’s database. Clearview says the technology “acts as a search engine of publicly available images.” Once Clearview matches the input photo to a photo in their database, Clearview provides a list of the websites where the matching input photos appear, called the “Image Index.” What distinguishes Clearview AI from other facial recognition systems is that the resulting links in the Image Index take a user to photos of people found on the open web rather than government-created records.


30 Id.; see also id. ("When a Clearview user uploads an image, Clearview’s proprietary technology processes the image and returns links to publicly available images that match the person pictured in the uploaded image.").


32 See Kashmir Hill, Unmasking a Company That Wants to Unmask Us All, N.Y. TIMES, https://www.nytimes.com/2020/01/20/reader-center/insider-clearview-ai.html [https://perma.cc/CV6V-UCX2] (Oct. 28, 2021) ("Clearview stuck out because it claimed to be scraping social media sites and the open web instead of using mugshots or D.M.V. photos, as was the norm with the other vendors.").

alleging Clearview violated their terms of service and demanded Clearview to stop using their photos without success.34 Regardless, Clearview’s database continues to grow, currently containing over thirty billion faces—all of it scraped from the Internet.35

1. Clearview’s Claim That Their Database Only Uses “Publicly Available Images” Requires Context

This section will demonstrate the power of a facial recognition system that can match input photos to photos scraped from the Internet by examining Yandex, a Russian version of Google36 that can match input photos to faces found on Vkontakte (“VK”), a Russian version of Facebook.37 Aric Toller, a journalist for Bellingcat, took a screenshot of a person (“Person A”) in the background of a YouTube video and uploaded it to Yandex, where he received a link to a VK post from a different person (“Person B”) that featured Persons A and B.38 Further, it is likely Clearview AI can similarly identify people from photos they don’t intend to upload; for example, if a “friend of yours posts a picture of you together at high school, once Clearview has snapped a picture of your face, it will create a permanent biometric print of your face” in their database.39 Importantly,

38 See Vox, supra note 37.
39 Katherine Tangalakis-Lippert, Clearview AI Scraped 30 Billion Images from Facebook and Other Social Media Sites and Gave Them to Cops: It Puts Everyone into a
Clearview AI can make matches to many more websites than just Facebook.\textsuperscript{40}

On March 13, 2020, pursuant to the California Consumer Privacy Act,\textsuperscript{41} Thomas Smith sent Clearview a request to provide the data they collected on him.\textsuperscript{42} He estimated Clearview retrieved his profile in under a minute,\textsuperscript{43} and he stated that “[t]he depth and variety of data that Clearview has gathered on me is staggering.”\textsuperscript{44} The Image Index contained a link to a story published about Mr. Smith by his “alma mater’s alumni magazine from 2012, and a follow-up article published a year later.”\textsuperscript{45} It also included his profile page from an online group “that [he] had forgotten [he] belonged to” and a link to a personal blog he started with his wife.\textsuperscript{46} Clearview provided the URL of his Facebook page, including the names of people with connections to him, like a faculty advisor and family member.\textsuperscript{47}

From this data, Smith stated that “an investigator . . . would know [his] name. They would also know where [he] went to school, what line of work [he is] in, and the region where [he] live[s]” all of which “was retrieved using a single image of [his] face.”\textsuperscript{48} Clearview AI doesn’t just turn a face into a nametag—it turns it into a biography.

In the example above, Smith’s Facebook profile was public;\textsuperscript{49} however, that does not mean private accounts are safe from


\textsuperscript{41} See CAl. CIV. CODE § 1798.100(b) (Deering 2024).

\textsuperscript{42} See Smith, \textit{supra} note 40.

\textsuperscript{43} See id.

\textsuperscript{44} Id.

\textsuperscript{45} Id.

\textsuperscript{46} See id.

\textsuperscript{47} Id.

\textsuperscript{48} Id.; see also Gershgorn, \textit{supra} note 6.

\textsuperscript{49} See Smith, \textit{supra} note 40.
Clearview’s database. New York Times journalist Kashmir Hill asked the CEO of Clearview AI to conduct a search of her and learned that Clearview had around 160 photos of her, ranging from professional headshots she knew about to photos she “didn’t realize were online.”\(^{50}\) One of the photos Clearview had of Hill was posted by a third party with someone walking in the background.\(^{51}\) At first glance, Hill could not see herself in the photo, but eventually “recognized the coat of the person in profile walking by in the background . . . a coat [she] bought in Tokyo;” Hill could not recognize herself in the photo—but Clearview could.\(^{52}\)

C. Most Americans Are in Clearview’s Database

Most Americans are probably in Clearview’s database, even if they do not know it.\(^{53}\) Clearview can collect photos containing your face from Instagram and/or Facebook photos in which you were tagged.\(^{54}\) This is still true even if you “un-tag yourself or later set your account to private;”\(^{55}\) once Clearview has scraped the photo, it stays in their database.\(^{56}\) Even if you set your Instagram or Facebook profile to private, your profile pictures on both sites (as well as your Facebook cover photo) are public without any option to make them private, so Clearview can scrape them.\(^{57}\) Additionally, Clearview


\(^{51}\) See id. (“I remember this one photo of somebody, and there’s a person walking by in the background. And when I first looked, I didn’t see me. Then I recognized the coat of the person in profile walking by in the background. It’s a coat I bought in Tokyo, very distinctive. And I was like, ‘Wow, that’s me.’”).

\(^{52}\) Id.

\(^{53}\) See LastWeekTonight, *supra* note 11, at 15:00.

\(^{54}\) See Gershgorn, *supra* note 6.

\(^{55}\) LastWeekTonight, *supra* note 11, at 15:11.

\(^{56}\) See Kashmir Hill, *The Secretive Company That Might End Privacy As We Know It*, N.Y. TIMES, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/92C6-4MZV] (Nov. 2, 2021) (“The company keeps all the images it has scraped even if they are later deleted or taken down . . . ”). In California, consumers can request a company to provide the data they have on them and demand that the company delete it; however, this requires proactive effort by the consumer. See CAL. CIV. CODE § 1798.100 (Deering 2024).

\(^{57}\) See Gershgorn, *supra* note 6.
has scaped some photos from “a collection of utterly bizarre and seemingly random websites” unrelated to the website where the photo was originally posted.\textsuperscript{58} Individuals from California, Colorado, Connecticut, Utah, and Virginia can request Clearview AI to delete their information from Clearview’s database,\textsuperscript{59} but ironically this requires the individual to give Clearview AI a photo of themselves.\textsuperscript{60}

\textbf{D. Police Are Using Clearview Search Results to Support Warrants}

In a leaked memo, Clearview AI states that any results provided through a Clearview AI search “are not intended or designed to be used as evidence in court, whether for purposes of demonstrating probable cause to obtain a warrant or otherwise.”\textsuperscript{61} However, this Section shows that despite this goal, police are using Clearview AI to obtain warrants.

The CEO of Clearview AI said the software’s results should be treated like “leads for law enforcement” or an “anonymous tip” from the public, but the reality is that law enforcement agencies are using Clearview AI to support warrant applications.\textsuperscript{62} For example, police in Evansville, Indiana have used Clearview AI to “conclusively

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{58} Merlan, supra note 31 (providing “Insta Stalker—one of dozens of sketchy Instagram scrapers available online,” as an example of one such bizarre website). An Instagram scraper is a software tool designed to automatically extract “specific web content (text, pictures, links)” directly from the website. See, \textit{e.g.}, The Best Instagram Scrapers for 2024, MAGICAL, https://www.getmagical.com/blog/instagram-scraper#:~:text=Scraping%20Instagram%20involves%20leveraging%20these,use%20an\%20Instagram\%20Profile\%20Scraper (last visited Apr. 17, 2024).
\item \textsuperscript{59} See Privacy & Requests, CLEARVIEW AI, https://www.clearview.ai/privacy-and-requests [https://perma.cc/84DR-FELG].
\item \textsuperscript{60} See, \textit{e.g.}, Clearview AI Privacy Webform, ONETRUST, https://privacyportal.onetrust.com/webform/1fd17ee-bd10-4813-a254-de7d5c09366a7c79caee5-6e86-4d8d-b409-7a932c09b942 [https://perma.cc/FR5Z-MCMV].
\item \textsuperscript{61} Clement Memorandum, supra note 29, at 2.
\end{itemize}
\end{footnotesize}
identify crime suspects” to support arrest affidavits.\textsuperscript{63} In total, the Evansville Police Department cited Clearview AI or facial recognition technology at least ten times in arrest affidavits related to shoplifting or theft cases between 2021 to 2023.\textsuperscript{64} Worryingly, detectives from the Evansville Police Department assert they are “under no obligation to disclose their use of facial recognition technology in arrest affidavits.”\textsuperscript{65} Furthermore, there are currently no federal laws regulating law enforcement’s use of Clearview AI “to generate leads,”\textsuperscript{66} and officers use the software when on patrol to identify people in real time, according to Police Chief Bolin of the Evansville Police Department.\textsuperscript{67}

Police use Clearview because the technology is better than the alternatives. For example, police officers in Gainesville, Florida prefer Clearview’s app over FACES, a state-provided facial recognition tool with a database of 30 million photos drawn from mug shots and Department of Motor Vehicle photos.\textsuperscript{68} They stated that Clearview’s “nationwide database of images is much larger, and unlike FACES, Clearview’s algorithm doesn’t require photos of people looking straight at the camera.”\textsuperscript{69}

Clearview provides police departments with a cheap and powerful investigative tool, which they have been quick to adopt. For

\footnotesize

\textsuperscript{63} Id.
\textsuperscript{64} See id.
\textsuperscript{65} Id.
\textsuperscript{67} See Harwood, supra note 62.
\textsuperscript{68} See Hill, \textit{Secretive Company}, supra note 56.
\textsuperscript{69} See id.
example, using Clearview, Indiana State Police solved a case within twenty minutes.\textsuperscript{70} Two men had gotten into a fight in a park, which ended with one man shooting the other in the stomach.\textsuperscript{71} Indiana police had a still image of the gunman’s face because a bystander recorded the crime on their phone.\textsuperscript{72} The police input this photo into Clearview, which provided them with a match almost instantaneously.\textsuperscript{73} The link associated with the database photo was from a video someone posted on social media, which included the suspect’s name in the caption of the video; importantly, the suspect “did not have a driver’s license and hadn’t been arrested as an adult, so he wasn’t in government databases.”\textsuperscript{74} Despite this, the police were able to arrest and charge the man based on the Clearview search result.\textsuperscript{75}

II. THE FOURTH AMENDMENT ADAPTS TO NEW TECHNOLOGY

Police departments around the country, such as those in Indiana and Florida,\textsuperscript{76} are using Clearview to support warrants because it is such a powerful investigative tool; however, the public safety benefits Clearview provides must be balanced against every citizen’s Fourth Amendment protections against “arbitrary invasions by government officials.”\textsuperscript{77}

Part II of this Note argues that the Fourth Amendment has adapted over time to continue to provide protection as police obtain more technologically advanced investigative tools. Section II.A argues that at the time of drafting, the Fourth Amendment only concerned itself with physical trespass by law enforcement. Section II.B discusses early Fourth Amendment case law’s adherence to this original meaning. Sections II.A and II.B demonstrate that early

\textsuperscript{70} See id.
\textsuperscript{71} See id.
\textsuperscript{72} See id.
\textsuperscript{73} See id.
\textsuperscript{74} Id.
\textsuperscript{75} See id.
\textsuperscript{76} See supra Section I.D.
Fourth Amendment jurisprudence was intended only to protect against physical trespass. Section II.C discusses how the Supreme Court departed from this reasoning in *Katz v. United States* to extend Fourth Amendment protections outside the home to cover society’s changed reasonable expectation of privacy in response to new technologies.\(^\text{78}\)

Sections II.D and II.E look at recent Fourth Amendment cases decided in the context of digital technology. Section II.D argues that the Court has extended Fourth Amendment protections when new technology provides police with the capability “to circumvent natural human privacy barriers.”\(^\text{79}\) Section II.E contends that the Court recognizes the distinct capabilities of digital surveillance technology to bypass innate human privacy safeguards, making previous Fourth Amendment case law pertaining to analog technology less relevant.

**A. The Fourth Amendment Was Originally Only Concerned With Physical Trespass**

Analysis of the precursors to the Fourth Amendment reveals that the founding generation’s primary concern was physical trespass from government officials. For example, in James Otis Jr.’s 1761 argument against general warrants in the high court of Massachusetts, he condemned general warrants for violating the “essential principle of English liberty that a peaceable man’s house is his castle.”\(^\text{80}\) Otis Jr.’s speech inspired “John Adams’s framing of Article XIV of the Massachusetts Declaration of Rights of 1780,” which in turn inspired “James Madison’s introduction of the proposal that became the Fourth Amendment [in the U.S. Constitution].”\(^\text{81}\) In 1763, a series of lawsuits stemmed from John Wilkes’ arrest for insulting

\(^{78}\) See generally *Katz v. United States*, 389 U.S. 347 (1967). See also *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (“[T]he same technological advances that have made possible non-trespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations.”).


\(^{81}\) *Id.* at 85; see also *Carpenter*, 585 U.S. at 303–04 (“In fact, as John Adams recalled, the patriot James Otis’s 1761 speech condemning writs of assistance was ‘the first act of opposition to the arbitrary claims of Great Britain’ and helped spark the Revolution itself.”).
the king’s speech further extended this reasoning. The first of these cases, *Huckle v. Money*, established the doctrine that crown officers are liable for *trespass* resulting from an unlawful search. Leonard Levy, an influential Constitutional scholar and historian, contends that “the Fourth Amendment, as well as the First and Fifth, owe[] something to the Wilkes cases.”

Both Otis’ statements and the Wilkes cases demonstrate that in the late 1700s, early American revolutionaries were—and could only be—concerned with physical trespass because there existed no technologies at the time that provided a way for law enforcement to intrude on an individual’s privacy absent trespass.

### B. Twentieth Century Supreme Court Holdings Limited Fourth Amendment Protections to Physical Tresspass

Twentieth century Supreme Court jurisprudence adhered to the Fourth Amendment’s original physical trespass interpretation. For instance, in *Olmstead v. United States*, four federal prohibition officers monitored Olmstead’s office phone by tapping phone lines in the basement of the building. Officers also tapped the phone lines on the streets near the houses of alleged co-conspirators. Importantly, in both instances, the wire taps were placed “without [physical] trespass upon any property of the defendants.”

The Court held that even a liberal construction of the Fourth Amendment could not cover telephone wires “reaching . . . the

---

82 See Levy, supra note 80, at 86.
83 See id. at 87–88 (“Chief Justice Charles Pratt said, when charging the jury: ‘To enter a man’s house by virtue of a nameless warrant, in order to procure evidence, is worse than the Spanish Inquisition, a law under which no Englishman would wish to live an hour.’”).
84 See id. at 79 (Leonard Levy is a Pulitzer Prize historian, Andrew W. Mellon All Claremont Professor of History, and Humanities, Emeritus, Claremont Graduate School.
85 See also David L. Hudson, Jr., *Leonard Levy*, FREE SPEECH Center (Feb. 18, 2024), https://firstamendment.mtsu.edu/article/leonard-levy/ [https://perma.cc/QSP6-P3ZR].
86 Id.
87 See Steven C. Douse, *The Concept of Privacy and the Fourth Amendment*, 6 U. Mich. J.L. REFORM 154, 159 (1972) (“A man’s confidences could be penetrated only by the naked eye or ear, and his property invaded only by physical entry or appropriation.”).
89 Id. at 457.
whole world” because those wires were outside the home; thus, any intrusion on them did not constitute “an actual physical invasion of [the] house.”\textsuperscript{90} The Court reasoned an individual who installs a telephone in their home accepts the risk their calls may be monitored because the telephone signals transmit along wires outside the individual’s property.\textsuperscript{91} Even during the twentieth century, this strict interpretation worried some Justices. For example, Justice Brandeis’ dissent expressed unease, anticipating that progress in science would provide the government with capabilities to effect searches without relying on breaking and entering, which was the Fourth Amendment’s contemplated method of effecting searches.\textsuperscript{92} “Can it be that the Constitution affords no protection against such invasions of individual security?”\textsuperscript{93}

C. The Court Has Expanded Fourth Amendment Protections to Cover More Than Physical Trespass to Protect Society’s Changed Expectation of Privacy

Thirty-nine years after \textit{Olmstead}, the Court confronted the constitutionality of an electronic listening and recording device attached to the outside of a public telephone booth in \textit{Katz v. United States}.\textsuperscript{94} The decision in \textit{Katz} broadened Fourth Amendment protections to protect this publicly accessible space to preserve society’s changed reasonable expectation of privacy.\textsuperscript{95}

The Court modified its prior trespass-focused Fourth Amendment analysis by shifting the focus from places to people.\textsuperscript{96} The Court found that one who goes into a phone booth and shuts the door behind them is entitled to assume that the conversation is private.\textsuperscript{97}

\textsuperscript{90} \textit{Id.} at 465–66.
\textsuperscript{91} See \textit{id.} at 466 (“The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment. Here those who intercepted the projected voices were not in the house of either party to the conversation.”).
\textsuperscript{92} See \textit{id.} at 473–74 (Brandeis, J., dissenting).
\textsuperscript{93} \textit{Id.} at 474.
\textsuperscript{94} 389 U.S. 347 (1967).
\textsuperscript{95} See \textit{id.} at 353.
\textsuperscript{96} See \textit{id.} at 351 (“For the Fourth Amendment protects people, not places.”).
\textsuperscript{97} See \textit{id.} at 352.
The Court found that “[w]hat a person knowingly exposes to the public, even in his own home or office, is not [protected by the] Fourth Amendment. . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”\(^9\) Justice Harlan’s concurrence, now the law,\(^9\) stated that Fourth Amendment protection required (1) a person to have “an actual (subjective) expectation of privacy, and (2) that the expectation is “one that society is prepared to recognize as ‘reasonable.’”\(^10\) The critical fact for Justice Harlan was that the defendant in *Katz* shut the door behind him, and in doing so turned the booth into “a temporarily private place whose momentary occupants’ expectations of freedom from intrusion are recognized as reasonable.”\(^10\) The Court’s holding in *Katz* reveals that a narrow reading of the Fourth Amendment would “ignore the vital role that the public telephone [had] come to play in private communication.”\(^10\) Put simply, the Court recognized that the ubiquity of the public telephone in modern society did not negate society’s reasonable expectation of privacy in their phone calls, even though the calls now could take place in a publicly accessible space.

The *Katz* decision reveals that (1) the Court’s Fourth Amendment analysis has changed before in response to widespread adoption of technology, and (2) society can retain a reasonable expectation of privacy even in publicly accessible spaces.\(^10\) Essentially, the Court recognized that a new technology had become so ingrained in people’s lives while providing the government the opportunity to affect searches without relying on the traditional methods

\(^9\) *Id.* at 351 (citations omitted).

\(^9\) *See* Smith v. Maryland, 442 U.S. 735, 740 (1979).

\(^10\) *Katz*, 389 U.S. at 361 (Harlan, J. concurring).

\(^10\) *Id.*

\(^10\) *Id.* at 352.

\(^10\) *Cf.* United States v. U.S. Dist. Ct. for E.D. of Mich., 407 U.S. 297, 313 (1972) (“Though physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed, its broader spirit now shields private speech from unreasonable surveillance.”).
contemplated during the Fourth Amendment’s drafting.\footnote{See generally \textit{Katz}, 389 U.S. 347; see also \textit{Olmstead}, 277 U.S. at 473–74 (Brandeis, J., dissenting) (predicting that future technological advances will “furnish the government with [more] means of espionage,” so Fourth Amendment protection should be broadened to account for that).} This reinforces the validity of Justice Brandeis’ words articulated in \textit{Olmstead} that to allow the government to intrude in this space unchecked would be “[t]o declare that in the administration of the criminal law the end justifies the means,” which runs counter to the Fourth Amendment’s purpose.\footnote{\textit{Olmstead}, 277 U.S. at 485.}

\textbf{D. The Court has Expressed Concern when New Technology Provides Law Enforcement with a “Superpower” that Triggers Fourth Amendment Protections}

To be clear, Section II.C does not stand for the proposition that all new technological advancements coincide with a new expectation of privacy. Technological advancements can decrease society’s expectation of privacy, but as discussed in this section, there is a limit to this decrease, particularly in the context of advancements in surveillance technology. In \textit{California v. Ciraolo}\footnote{476 U.S. 207 (1986).} and \textit{Kyllo v. United States},\footnote{533 U.S. 27 (2001).} the U.S. Supreme Court considered the extent to which new surveillance technology can diminish a society’s reasonable expectation of privacy. If there is a limit to the extent that analog surveillance can decrease society’s expectation of privacy, then new digital surveillance technology must also be subject to that same limitation.

In \textit{Ciraolo}, the Supreme Court confronted whether there was a reasonable expectation of privacy from aerial observation of the curtilage of a home conducted from public airspace.\footnote{See \textit{California v. Ciraolo}, 476 U.S. 207, 209 (1986).} Law enforcement officers conducted aerial observation of the defendant’s backyard from a fixed-wing aircraft at an altitude of 1,000 feet and observed marijuana plants growing within it.\footnote{See \textit{id}.}
To fully understand the holding in California v. Ciraolo, context regarding the airline industry during the 1980s is necessary. In 1971, only 49% of Americans reported they had flown on a plane, but by 1989, that number increased to 78%. Air travel had become ubiquitous in American life. The Court in Ciraolo noted that the aircraft in question was flying in public airspace; thus, “any member of the public flying in this airspace who glanced down could have seen everything the officers observed.” The officers or the public could theoretically observe the marijuana plants with the naked eye. Subsequently, the Court found no Fourth Amendment violation because, it reasoned, there was no reasonable expectation of privacy from such observations.

The reasoning raises more questions than answers. Is it unreasonable for an individual to have a reasonable expectation of privacy from snooping aircraft flying at 1,000 feet by correctly assuming most of the public flies at an altitude much higher? Put differently, does an individual forfeit all expectation of privacy from snooping conducted from public spaces? The Court confronted this question in Kyllo v. United States.

In Kyllo, law enforcement used a thermal imaging device from a public street to detect the heat signatures emanating off of a house, and the Supreme Court ruled that this was a search. Notably, the fact the surveillance was conducted from a public street was considered irrelevant. Rather, the court highlighted that the thermal imaging technology was not in public use and it allowed officers to

---

111 Id. at 213–14.
112 See id. at 215 (“The Fourth Amendment simply does not require the police traveling in the public airways at this altitude to obtain a warrant in order to observe what is visible to the naked eye.”).
115 See generally id.
116 Id. at 33.
infer some details about the inside of the home, which is traditionally the most protected area of privacy under the Fourth Amendment. The Court held law enforcement’s use of this sensory-enhancing technology to gather information about the interior of the home (which could not otherwise have been obtained without physical intrusion) constituted a search.

Why is surveillance of a backyard from public airspace using an aircraft not a search but a thermal scan conducted from a public street is? The Court in Kyllo reasoned that the thermal scan revealed only “crude visual image[s] of the heat being radiated”; it “did not show any people or activity” inside the house. Yet, the Court still found that an individual still has a reasonable expectation of privacy in the heat emanating from their house. Some rightly contend the different outcomes are because the Court is more concerned when the technology does not just “augment ordinary human capabilities,” but instead provides law enforcement with the ability to “circumvent natural human privacy barriers.”

The Fourth Amendment is unconcerned with technological enhancements of ordinary human senses, such as the technology at issue in Ciraolo. For example, in United States v. Knotts, officers placed a beeper (i.e., a radio transmitter) in a container—this allowed them to track the physical location of the container to the defendant’s residence (i.e., officers followed the radio signal emanated by the beeper from their cars). Importantly, “the movements of the automobile and the arrival of the can containing the beeper in the area of the cabin could have been observed by the naked eye,”

---

117 See id. at 34.
118 See id. (“[I]n the case of the search of the interior of homes—the prototypical . . . area of protected privacy—there is a ready criterion, with roots deep in the common law.”).
119 See id.
120 Compare Ciraolo, 476 U.S. at 207, with Kyllo, 533 U.S. at 27.
121 Kyllo, 533 U.S. at 30; see also id. at 37 (“The Fourth Amendment’s protection of the home has never been tied to measurement of the quality or quantity of information obtained.”).
122 Ferguson, supra note 79, at 31–32 (2022).
123 See, e.g., Dow Chem. Co. v. United States, 476 U.S. 227, 228 (1986) (“The mere fact that human vision is enhanced somewhat, at least to the degree here, does not give rise to constitutional problems.”).
and therefore, no Fourth Amendment violation occurred.\textsuperscript{125} This remained true even though the officers only conducted “partial visual surveillance as the automobile containing the [beeper] moved along the public highways.”\textsuperscript{126} Essentially, the beeper allowed the officers to more efficiently survey the vehicle, but the Court emphasized that they were still using ordinary human senses to track the vehicle.\textsuperscript{127} As was the case in \textit{Ciraolo}, the officers were still relying on ordinary visual senses, albeit from an enhanced viewpoint.\textsuperscript{128}

A year later, the Court held in \textit{United States v. Karo} that officers using the same beeper technology used in \textit{Knotts} to locate a container inside a residence was a Fourth Amendment violation.\textsuperscript{129} The critical distinction was that the officers in \textit{Karo} “did not maintain tight surveillance [of the target] for fear of detection,” instead relying on the beeper to determine that the container was inside the premises.\textsuperscript{130} The fact that the beeper was inside the house and that the officers could not have visually verified that fact because they did not maintain a visual line of sight is what caused the Fourth Amendment violation.\textsuperscript{131} The officers in \textit{Karo} possessed the ability to confirm what they could not have seen with their eyes (i.e., the officers knew the container was in the house even though they could not have seen the container go inside the house). This ability circumvented a natural privacy barrier: the walls of the house. Likewise, the officers in \textit{Kyllo} were not just more efficient in their surveillance by detecting heat signatures emanating off the house, they also possessed the ability “to circumvent natural human privacy barriers” by seeing through walls.\textsuperscript{132} The Court’s decision in \textit{Kyllo} reflects an adaptation of Fourth Amendment principles to modern


\textsuperscript{126} \textit{Id.} at 713 (citing generally \textit{Knotts}, 460 U.S. 276 (1983)).

\textsuperscript{127} See \textit{Knotts}, 460 U.S. at 284; see also \textit{Leaders of a Beautiful Struggle v. Balt. Police Dep’t}, 2 F.4th 330, 340 (4th Cir. 2021) (“[I]f ‘dragnet type law enforcement practices . . . should eventually occur,’ then ‘different constitutional principles may be applicable.’”) (quoting \textit{Knotts}, 460 U.S. at 284)).

\textsuperscript{128} See \textit{Ferguson}, supra note 79, at 31.

\textsuperscript{129} See \textit{Karo}, 468 U.S. at 714.

\textsuperscript{130} \textit{Id.} at 709–10.

\textsuperscript{131} See \textit{id.} at 715.

\textsuperscript{132} \textit{Ferguson}, supra note 79, at 31–32.
society, where new surveillance technology necessitates a reevaluation of society’s reasonable expectation of privacy.\footnote{133 Cf. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (“[T]he same technological advances that have made possible nontrespassory surveillance techniques will also affect the Katz test by shaping the evolution of societal privacy expectations.”).}

\textbf{E. The Court Has Acknowledged Digital Surveillance Possesses Unique Characteristics, Making It Capable of Circumventing Traditional Human Privacy Barriers}

The rise of the digital age has provided law enforcement with new, powerful digital surveillance tools.\footnote{134 See Ali Watkins, \textit{How the N.Y.P.D. Is Using Post-9/11 Tools on Everyday New Yorkers}, \textit{N.Y. Times}, https://www.nytimes.com/2021/09/08/nyregion/nypd-9-11-police-surveillance.html (June 22, 2023) (“The police acknowledged their use of a vast network of license plate readers, thousands of surveillance cameras, mobile X-ray vans and digital tools that are used to scrub social media profiles and retain deleted information.”).} In response to this development, the Supreme Court has delineated the unique characteristics of digital surveillance that trigger Fourth Amendment protections. Section II.E will explore those characteristics by looking at the concurring opinions in \textit{United States v. Jones},\footnote{135 See generally \textit{Jones}, 565 U.S. at 413–18 (Sotomayor, J., concurring); \textit{Jones}, 565 U.S. at 418–31 (Alito, J., concurring).} along with the Court’s other decisions regarding the applicability of prior Fourth Amendment doctrine to digital technology.

In \textit{Jones}, a GPS device placed on a suspect’s vehicle allowed law enforcement to remotely monitor the vehicle’s movements on public roads.\footnote{136 See \textit{id.} at 403 (majority opinion) (“[T]he Government used the device to track the vehicle’s movements, and once had to replace the device’s battery when the vehicle was parked in a different public lot in Maryland. By means of signals from multiple satellites, the device established the vehicle’s location within 50 to 100 feet, and communicated that location by cellular phone to a Government computer. It relayed more than 2,000 pages of data over the 4-week period.”).} The Court previously held in \textit{Knotts} that a person does not have a reasonable expectation of privacy in their movement on public thoroughfares because such information was “voluntarily conveyed to anyone who wanted to look,”\footnote{137 United States v. Knotts, 460 U.S. 276, 281 (1983); see also \textit{id.} at 283–84 (hinting at the possibility that dragnet surveillance may require a different result).} but this logic was not extended to the GPS tracker in \textit{Jones}.\footnote{138 See \textit{Jones}, 565 U.S. at 430 (Alito, J., concurring).} The digital GPS tracking in...
Jones allowed for precise and continuous tracking of the vehicle’s movements for a period of four weeks. In contrast, the beeper in Knotts emitted periodic radio signals law enforcement could follow, but it did not provide continuous location data. Instead, the Knotts beeper assisted visual surveillance as officers followed the suspect’s vehicle to its destination while augmenting the officers’ ability to maintain sight of the vehicle in traffic (i.e., the beeper helped the officers see the car they were following). In Jones, five concurring Justices recognized the digital nature of modern GPS tracking gave it unique characteristics making it especially invasive. Unlike radio signals, the digital data captured by GPS trackers could be stored indefinitely and mined for information years into the future (and much cheaper than analog surveillance techniques like having officers tail the car). Society’s expectation has been that law enforcement would not (and simply could not) monitor and catalog every single movement of an individual’s car for a long period because it would be too resource intensive. In Jones, five concurring Justices hinted that because digital technology allows law enforcement to capture, store, and retroactively analyze a large amount of data, society can possess a reasonable expectation of privacy from that technology.

139 Id.
140 See Knotts, 460 U.S. at 277.
141 See id. at 278 (“During the latter part of this journey, [the car] began making evasive maneuvers, and the pursuing agents ended their visual surveillance. At about the same time officers lost the signal from the beeper, but with the assistance of a monitoring device located in a helicopter the approximate location of the signal was picked up again about one hour later.”).
142 See id.
143 See Jones, 565 U.S. at 415–17 (Sotomayor, J., concurring); see also id. at 429 (Alito, J., concurring) (“Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap.”).
144 See id. at 415–16 (Sotomayor, J., concurring).
145 See id. at 430 (Alito, J., concurring).
146 See id. at 416 (Sotomayor, J., concurring) (“The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person . . .”); see also id. at 429 (Alito, J., concurring) (“The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial
accurately collect the public location of a vehicle for a long period of time infringed on what was a natural human privacy barrier: the resource cost for police to conduct such surveillance.

The Court has recognized the unique capabilities of digital technology renders some analog-based precedent, like the third-party doctrine, inapplicable to digital surveillance technology. In *Smith v. Maryland* and *Carpenter v. United States*, the Court considered the applicability of the third-party doctrine to cell phone data. In *Smith*, the Supreme Court held that individuals do not have a reasonable expectation of privacy in the numbers dialed from their private telephones. The Court reasoned that by dialing numbers and transmitting them to the telephone company, the individual voluntarily shared the information with a third party, thus assuming the risk the third party would reveal the information to the government—this is called the third-party doctrine.

Contrastingly, in *Carpenter*, the Court found individuals do retain an expectation of privacy in the whole of their physical movements as captured through Cell Site Location Information (“CSLI”). CSLI data is the time-stamped record of each time the cell phone connected to a cell tower, which reveals the phone’s location. Importantly, the reasoning in *Smith* could apply to CSLI data—an individual voluntarily purchases a cell phone, and the cell-phone must generate CSLI to operate. Thus, the question is: why

---

148 See *Smith*, 442 U.S. at 745–46.
149 Id. at 744.
150 See *Carpenter* 585 U.S. at 307–08.
151 Id. at 309–10.
152 See id. at 301.
doesn’t the voluntary decision to purchase a cell phone come with an assumption of the risk that the cellphone company would reveal the CSLI data to the government?

The government in Carpenter argued cell site records were “business records” created and maintained by the wireless carriers and the government’s access to those records was not a search.\footnote{Carpenter, 585 U.S. at 313.} The Court flatly rejected this argument, noting the Government’s argument failed to contemplate “the seismic shifts in digital technology that made possible the tracking of not only [the defendant’s] location but also everyone else’s.”\footnote{Id. at 310.} The Court explicitly stated that “a person does not surrender all Fourth Amendment protection by venturing into the public sphere.”\footnote{Id. at 310.} Once again, the Court was particularly concerned about how easily, cheaply, and efficiently the government could retrieve “an intimate window into a person’s life” through CSLI data compared to analog surveillance tools like a pen register.\footnote{Id. at 311; see also id. (“With just the click of a button, the Government can access each carrier’s deep repository of historical location information at practically no expense.”).} Moreover, because CSLI data can be stored, the Court was concerned with the retrospective capabilities law enforcement would have to reconstruct a person’s movements, thereby eliminating previous limitations—previously, police efforts to re-trace a suspect’s movements “were limited by a dearth of records and the frailties of recollection.”\footnote{Id. at 312; see also id. (“With access to CSLI, the Government can now travel back in time to retrace a person’s whereabouts, subject only to the retention policies of the wireless carriers.”).} Essentially, police had a tool capable of following everyone everywhere and storing that information forever, giving them the ability to circumvent natural human privacy barriers (e.g., individuals’ “expectation has been [that the police] would not—and . . . simply could not—secretly monitor and catalogue every single movement of an [their] car for a very long period”).\footnote{See United States v. Jones, 565 U.S. 400, 430 (Alito, J., concurring).} Put simply, CSLI’s digital nature makes it uniquely invasive of privacy, which necessitated the narrowing of Smith’s broad principles.
The majority opinion in *Carpenter* signaled a departure from the strict application of doctrine decided in the context of analog technology, recognizing certain digital data deserves stronger protection due to its pervasive presence and revealing nature.\(^\text{160}\) It seems that the distinction between *Carpenter* and *Smith* lies in the evolution of societal norms regarding privacy,\(^\text{161}\) the nature of the technology involved,\(^\text{162}\) and the depth and breadth of personal information that can be gleaned from digital data.\(^\text{163}\) *Smith* involved a relatively limited data set—a list of phone numbers\(^\text{164}\)—while *Carpenter* involved a vast amount of data constantly being collected that could be retroactively analyzed to reveal intimate details, presenting far more serious privacy concerns.\(^\text{165}\)

These cases reveal that when digital data collection provides law enforcement the ability to (1) collect a near infinite amount of data that can (2) be stored indefinitely, and (3) the data reveals an intimate portrait into one’s life, the Fourth Amendment applies.

### III. Circuit Court Rulings Reveal the Fourth Amendment is Not Concerned with Digital Surveillance Systems that Are Targeted

This Part will analyze recent Circuit Court rulings which have wrestled with the Fourth Amendment’s application to more recent digital surveillance systems as they reveal the boundaries of permissible digital surveillance (i.e., when a digital surveillance system does not run afoul of the Fourth Amendment).

---

\(^\text{160}\) See *id.* at 320.

\(^\text{161}\) See *id.* at 309 ("[W]hen *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person’s movements.").

\(^\text{162}\) See *id.* at 313 ("The Government’s position fails to contend with the seismic shifts in digital technology . . .").

\(^\text{163}\) See *id.* at 320 ("In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.").


\(^\text{165}\) See *Carpenter*, 585 U.S. at 311–12.
In Leaders of a Beautiful Struggle v. Baltimore Police Department, the Fourth Circuit granted a preliminary injunction against the Baltimore Police Department’s Aerial Investigation Research ("AIR") program, holding it was likely a violation of the Fourth Amendment. The AIR program used multiple planes equipped with cameras, which captured roughly thirty-two square miles per image per second. The planes flew about forty hours a week, obtaining an estimated twelve hours of coverage of 90% of the city daily. Collection was limited to daylight hours, and the photographic resolution was limited to one pixel per person or vehicle. Importantly, the AIR program did not provide real-time analysis; it was purely retroactive (i.e., the images taken were analyzed to identify individuals and vehicles from a crime scene).

The district court rejected Plaintiff’s preliminary injunction because “the AIR pilot program [had] limited location-tracking abilities,” it “only depict[ed] individuals as miniscule dots moving about a city landscape,” and the planes did not fly around the clock; thus, the gaps in the data prohibited the tracking of individuals over multiple days, unlike the CSLI data in Carpenter or the GPS tracker in Jones. From that premise, the district court believed the AIR program did not expose the “privacies of life.”

On appeal, the Fourth Circuit found it was inconsequential that the AIR program only surveyed for twelve hours a day (which created gaps in the data) because the program still enabled photographic, perfect, and retrospective tracking of everyone in Baltimore. The Court applied the principles articulated in Carpenter.

---

167 See id. at 334.
168 See id.
169 See id.
170 See id.
171 Id. at 340.
172 See Carpenter v. United States, 585 U.S. 296, 312 (2018) (Allowing the government unchecked access to CSLI data means “[w]hoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years . . . ”).
174 Leaders of a Beautiful Struggle, 2 F.4th at 340.
175 See id. at 342.
and expressed concern about the AIR program’s dragnet surveillance capabilities.\footnote{See id. at 340–42 (“Law enforcement can ‘travel back in time’ to observe a target’s movements, forwards and backwards. Without technology, police can attempt to tail suspects, but AIR data is more like ‘attach[ing] an ankle monitor’ to every person in the city. ‘Whoever the suspect turns out to be,’ they have ‘effectively been tailed’ for the prior six weeks . . . Thus, the ‘retrospective quality of the data’ enables police to ‘retrace a person’s whereabouts,’ granting access to otherwise ‘unknowable’ information.” (quoting Carpenter, 585 U.S. at 312)).}

In contrast, the Seventh Circuit upheld a police department’s warrantless use of three video cameras attached to utility poles directed at an individual’s home.\footnote{See generally United States v. Tuggle, 4 F.4th 505 (7th Cir. 2021).} In United States v. Tuggle, officers placed three digital cameras on public utility poles for eighteen months.\footnote{See id. at 511.} “The first two cameras viewed the front of [the defendant’s] home and an adjoining parking area. The third camera also viewed the outside of the home but primarily captured a shed.”\footnote{Id. at 524.} The defendant challenged the use of the cameras, asserting that twenty-four-hour surveillance of his home was an unconstitutional search because such surveillance “captured the whole of [his] movements,”\footnote{See id.} which could reveal intimate details similarly to the GPS in Jones and the CSLI data in Carpenter.\footnote{See id. at 524.} The Seventh Circuit disagreed, upholding the constitutionality of these cameras because they didn’t expose “where [the defendant] traveled, what businesses he frequented, with whom he interacted in public, or whose homes he visited.”\footnote{Id.} Further, the Court found the cameras distinguishable from CSLI data because the cameras were targeted at a single individual at a discreet location,\footnote{Id.} while CSLI data applied to “396 million cell phone service accounts in the United States”\footnote{Carpenter v. United States, 585 U.S. 296, 300 (2018); see also Tuggle, 4 F.4th at 524 (“[T]he cameras . . . highlighted [the defendant’s] lack of movement, surveying only the time he spent at home and thus not illuminating what occurred when he moved from his home.”); Leaders of a Beautiful Struggle v. Balt. Police Dep’t, 2 F.4th 330, 345 (4th Cir. 2021) (distinguishing cases involving a discreet operation surveilling individual targets).} which was generated wherever the individual went.
Importantly, the Seventh Circuit did not rest its decision on the premise that the government “could have” achieved the same surveillance through physical means like “stationing an agent atop the utility poles outside [the defendant’s] home, thus rendering the decision to . . . use pole cameras constitutional.” The Court found such surveillance would really only be possible for a couple of days, and the fact officers technically could have physically surveyed the premises does not automatically make eighteen months of effortless surveillance constitutional. It reasoned that such a fiction “contravenes the Fourth Amendment and Katz’s command to assess [the] reasonableness” of government intrusion. Put differently, digital surveillance like pole cameras can be so efficient that its use “circumvent[s] natural human privacy barriers,” thereby triggering Fourth Amendment protections.

These two cases stand for the proposition that when a digital surveillance system can surveil large swaths of the population for long lengths of time, store the digital data indefinitely, and make it retroactively mineable, then the Fourth Amendment provides protections against law enforcement’s unchecked use of that digital surveillance system.

---

185 Tuggle, 4 F.4th at 526.
186 See id. (“We thus close the door on the notion that surveillance accomplished through technological means is constitutional simply because the government could theoretically accomplish the same surveillance—no matter how laborious—through some nontechnological means.”).
187 Id.
188 Ferguson, supra note 79, at 31–32.
189 See Tuggle, 4 F.4th at 526 (“To assume that the government would, or even could, allocate thousands of hours of labor and thousands of dollars to station agents atop three telephone poles to constantly monitor Tuggle’s home for eighteen months defies the reasonable limits of human nature and finite resources. In our view, the premise that the government could realistically accomplish the pole camera surveillance here for more than a few days is a fiction that courts should not rely on to limit the Fourth Amendment’s protections.”); see also United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).
IV. HOW CLEARVIEW AI IMPLICATES THE FOURTH AMENDMENT

This Part will show that Clearview AI is a digital surveillance system with many of the capabilities implicating Fourth Amendment protections. Section IV.A will argue Clearview’s legal argument is insufficient to justify the warrantless use of their technology. Sections IV.B and IV.C will demonstrate that an individual possesses a reasonable expectation of privacy in photos of themselves found on the Internet. Ultimately, this Part argues that when an individual exhibits an expectation of privacy in their online presence, the police should not be able to use a Clearview AI search to support a warrant application.

A. Clearview’s Legal Justification for the Warrantless Use of Their Technology Is Insufficient to Justify the Warrantless Use of Their Technology

In a leaked memo, Clearview defended the warrantless use of their technology on the premises that 1) the technology does not track a person’s physical movements, and 2) a person does not have a reasonable expectation of privacy in information voluntarily turned over to third parties. This Note argues neither premise is sufficient to justify the warrantless use of Clearview AI because 1) the Court’s concern with digital surveillance is not singularly focused on the tracking of physical movements, and 2) the Court has refused to extend prior precedent to new digital technologies in recognition of its special capabilities distinguishing it from past technologies.

First, Clearview argues that because the technology does not directly track a person’s physical movements, the Court’s concerns articulated in Carpenter are not implicated. However, the Court’s concern about law enforcement’s ability to track an individual’s physical movements stemmed from what was revealed through such surveillance. Access to the CSLI data allowed the government to easily, cheaply, efficiently, and retroactively retrieve “an intimate

190 See Clement Memorandum, supra note 29, at 4. In Carpenter v. United States, the Court found individuals do retain an expectation of privacy in the whole of their physical movements as captured through CSLI. See 585 U.S. 296, 310 (2018).

191 See Carpenter, 585 U.S. at 311 (“With just the click of a button, the Government can access each carrier’s deep repository of historical location information at practically no expense.”).
window into a person’s life.”\textsuperscript{192} Put simply, if the government can learn where everyone traveled with their cell phone, they then could learn an incredible amount of information about a person. Thus, the Court’s holding in Carpenter should not solely be restricted to digital surveillance that tracks physical movements; it should apply to all digital surveillance that allows the government to obtain easily and cheaply “an intimate window into a person’s life.”\textsuperscript{193} In contrast to CSLI data, the pole camera in Tuggle did not provide enough information about the Defendant to trigger Fourth Amendment protections.\textsuperscript{194} However, when the digital surveillance system reveals one’s high school, hometown, friends, hobbies, and vacation photos\textsuperscript{195} the Fourth Amendment should be implicated because the aggregation of such information would reveal to officers something “not actually exposed to public view,”\textsuperscript{196} which is the “wealth of detail about [an individual’s] familial, political, professional, religious, and sexual associations.”\textsuperscript{197}

Clearview’s second argument is that a person “has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”\textsuperscript{198} Clearview argues that because their technology compares the input image against “publicly available images” gathered from public facing websites, individuals do not have a reasonable expectation of privacy in images they voluntarily turned over to third parties.\textsuperscript{199} “The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another,”\textsuperscript{200} however, “diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely.”\textsuperscript{201} It is important to note

\textsuperscript{192} Id.
\textsuperscript{193} Carpenter, 585 U.S. at 311.
\textsuperscript{194} See id.
\textsuperscript{195} See Smith, supra note 40.
\textsuperscript{198} Clement Memorandum, supra note 29, at 3 (citing Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).
\textsuperscript{199} Id.
\textsuperscript{201} Riley v. California, 573 U.S. 373, 392 (2014).
Clearview’s position ignores the fact that most Fourth Amendment case law was decided in the context of analog surveillance technology, but the Court has repeatedly hinted analog precedent like the third-party doctrine may not be appropriate for digital technologies\textsuperscript{202} because digital is fundamentally different.\textsuperscript{203} In fact, the Court in \textit{Carpenter} explicitly warned against a rigid application of precedent like the third-party doctrine to modern society where most people’s data is stored by third parties.\textsuperscript{204}

\section*{B. Individuals Have a Reasonable Expectation of Privacy in Photos They Post}

Section IV.B will demonstrate that an individual maintains a reasonable expectation of privacy in photos posted to social media by said individual. First, for an expectation of privacy to exist, the individual must exhibit “an actual (subjective) expectation of privacy.”\textsuperscript{205} Thus, an individual can only maintain an expectation of privacy in social media accounts that are private, similar to how the phone booth must be closed for Fourth Amendment protections to apply.\textsuperscript{206} Again, though, one’s profile picture and cover photo on Facebook are public without any option to make it private, and private accounts on Instagram cannot hide profile pictures.\textsuperscript{207} This

\begin{footnotesize}
\begin{enumerate}
\item [\textsuperscript{202}] See Kate Weisburd, \textit{Sentenced to Surveillance: Fourth Amendment Limits on Electronic Monitoring}, 98 N.C. L. Rev. 717, 721 (2020) (“The Court has likewise recognized that the concept of a ‘reasonable expectation of privacy’ for Fourth Amendment purposes must reflect the ‘seismic shifts in digital technology’ that now allow for ‘near perfect surveillance’ of digital records that ‘hold for many Americans the “privacies of life.”’ ‘These efforts reflect a bipartisan consensus that, when it comes to government surveillance of private citizens, “digital is different.”’).
\item [\textsuperscript{203}] See Ferguson, supra note 79, at 26.
\item [\textsuperscript{204}] See Carpenter, 585 U.S. at 305 (“[W]e rejected in \textit{Kyllo} a ‘mechanical interpretation’ of the Fourth Amendment . . . .” (quoting \textit{Kyllo} v. United States, 533 U.S. 27, 35 (2001))); see also United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (“[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties . . . . This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.” (citations omitted)).
\item [\textsuperscript{205}] Smith v. Maryland, 442 U.S. 735, 740 (1979) (Harlan, J., concurring) (quoting \textit{Katz} v. United States, 389 U.S. 347, 361 (1967)).
\item [\textsuperscript{206}] See \textit{Katz}, 389 U.S. at 361 (Harlan, J. concurring).
\item [\textsuperscript{207}] See Gershgorn, supra note 6.
\end{enumerate}
\end{footnotesize}
means Clearview AI can scrape some photos even if an individual make their social media accounts private.

Clearview AI has indiscriminately collected and continues to collect photos on a broad swath of individuals who have no suspicion of wrongdoing.\(^{208}\) The capability to capture and store such a large amount of photos on the internet that can reveal an individual’s employment history, social media activity, and online transactions epitomizes “dragnet surveillance,” a style of surveillance that is broad, sweeping, and indiscriminate in what information it targets.\(^{209}\) Additionally, when all that data is aggregated, it reveals an incredible amount of detail about individuals.\(^{210}\)

A more difficult situation arises when the photos are scraped by Clearview AI when the individual’s account was public but subsequently set to private after the photos were scraped. Here, the individual still exhibits a subjective expectation of privacy by setting their accounts to private, because the individual took active steps to restrict access to their photos.\(^{211}\) The question, then, is whether an individual’s subjective expectation of privacy is reasonable. The individual does have a reasonable expectation of privacy because for courts to hold otherwise would greenlight dragnet surveillance with retroactive capabilities revealing to the government the intimacies of life.

First, the notion that a user knowingly exposes their information to the public by posting photos from a public account\(^ {212}\) ignores the


\(^{209}\) See Patel, *supra* note 50, at 23 (“Clearview AI . . . scraped billions of photos from the public internet. They now have 30 billion faces in their database collected from social media sites like Facebook, Instagram, LinkedIn, [and] Venmo.”).


\(^{211}\) For an example of the steps needed to make one’s account private on a social media platform, see *Make Your Instagram Account Private*, INSTAGRAM, https://help.instagram.com/448523408565555 [https://perma.cc/75L9-58HK] (last visited Apr. 10, 2024).

THE USE OF CLEARVIEW AI

2024] 1025

The retroactive nature of this data. The type of surveillance contemplated for this premise was discrete and targeted (i.e., a person did not have a reasonable expectation of privacy in what they knowingly exposed to the public when the police were watching). Clearview facilitates a much different style of surveillance that entails the government capturing and storing nearly every photo and the accompanying data anytime an individual posted to social media. Additionally, Clearview allows for those photos and accompanying data to be analyzed at any time. It’s as if the police were watching the individual the entire time, even though at the time the photo was harvested the individual was not suspected of any wrongdoing. In this situation, the government can remember nearly every photo the individual exposed to the public with perfect recall. Put differently, “[w]hoever the suspect turns out to be,” they have “effectively been tailed” and the “[p]olice need not even know in advance whether they want to follow a particular individual, or when.”

Additionally, this type of surveillance could not be conducted by law enforcement without Clearview AI—it would be cost prohibitive for police departments to obtain the information provided by Clearview AI using traditional investigative techniques, like having officers personally sift through an individual’s social media accounts. Clearview AI provides inexpensive dragnet surveillance with retroactive capabilities, which suggests that Fourth Amendment protections apply.

To be sure, this situation touches the boundaries of the third-party doctrine, but the doctrine should not be extended. First, the Supreme Court narrowed Smith’s broad third-party doctrine holding when applying it to digital surveillance because of the unique characteristics of digital surveillance systems. Thus, courts confronted with precedent (like the third-party doctrine), which was decided in


215 See Carpenter, 585 U.S. at 314.
the context of analog technology, should avoid a strict application of that doctrine.216

C. Individuals Have a Reasonable Expectation of Privacy in Photos of Themselves That Are Posted by Someone Else

Section IV.C will demonstrate that individuals maintain an expectation of privacy in photos of themselves posted to social media by someone else. An individual would still need to exhibit a subjective expectation of privacy to receive Fourth Amendment protections.217 Assuming the individual’s own social media accounts are private, the issue is whether the individual’s expectation of privacy in a photo of himself posted by another person is reasonable. Take the previously-discussed article from Kashmir Hill, where Clearview had a picture of Hill in Tokyo that someone else posted without Hill’s consent.218 This Note does not argue that a lack of consent always triggers Fourth Amendment protections, but allowing the police to seek a warrant against Hill based on the picture posted by a third-party picture is essentially a form of dragnet surveillance because the camera of the third-party who captured the photo of Hill in Tokyo has retroactively been turned into a government surveillance camera and thus, should trigger the Fourth Amendment.

If, for example, Clearview scraped the public Instagram account of a wedding photographer that has an individual in the background of a picture, or that individual’s friend posted a picture of both of them from high school without asking for consent, Clearview AI can obtain those photos.219 Additionally, all of these photos can be retroactively analyzed at any point in the future. Clearview AI has turned every digital camera and smartphone into a government surveillance camera. This Note argues that this is prototypical dragnet surveillance. The ability to cheaply capture, store, and retroactively analyze every photo taken of an individual by other people should be impermissible under the Fourth Amendment. Law enforcement would not and simply could not monitor and catalog every single

216 See id. at 320.
217 See id. at 740.
218 See discussion supra Section I.C; Patel, supra note 50.
219 See Tangalakis-Lippert, supra note 39.
photo taken of an individual by others because it would be too resource intensive, echoing the Court’s reasoning in *Jones*. Further, the only way anyone could avoid being included in Clearview AI’s database is to set all social media accounts to private and avoid every digital camera and smartphone, which is likely an impossible task in today’s age. Thus, Clearview AI allows the government to attach an “ankle monitor” to its own citizens without Fourth Amendment protections.

**CONCLUSION**

Can we possess a reasonable expectation of privacy in an ever more connected world? To answer that, it’s important to remember that social media platforms were “built to facilitate the posting of public information, and social media platforms entrenched this idea; Facebook recruited a billion users between 2009 and 2014, when posting publicly . . . was [Facebook’s] default setting.” Did 243.58 million American citizens give up their expectation of privacy by creating a Facebook account? If they did, what about those who set their accounts to private but whose profile pictures and cover pictures are forced to be publicly displayed? Clearview harvested nearly thirty billion photos from the most popular platforms by violating those platforms’ terms of service, and in so doing has likely de-anonymized countless Americans. This represents an enormous shift in our offline lives where we control “who we introduce ourselves to” and how much of ourselves we reveal. Ultimately, this Note focuses on whether we can have a reasonable expectation of privacy from the police in our online lives.

---

222 Gershgorn, supra note 6.
223 See McCain, supra note 3.
224 See Gershgorn, supra note 6.
The Fourth Amendment has always adapted to changing technology. More specifically, the Fourth Amendment has adapted to society’s changed expectation in privacy as technology advances. The Supreme Court has recognized the profound danger digital surveillance presents to American liberty and has articulated the specific capabilities that make digital surveillance run afoul of the Fourth Amendment. Clearview AI is such a digital surveillance system, because it provides law enforcement with the ability to survey a large swathe of the population and collect a near infinite amount of data, capable of being stored indefinitely and revealing an intimate portrait into one’s life.

The purpose of this Note is not to argue that an individual has a reasonable expectation of privacy in everything they post on the Internet. To be sure, it is unlikely an individual can claim an expectation of privacy in cases like Thomas Smith’s personal blog on a public-facing website,\(^\text{227}\) but there is no setting on Clearview’s platform to filter out links to images in which an individual does have a reasonable expectation of privacy. The presence of Smith’s blog link in Clearview AI’s search results should not grant police access to such a powerful tool without the authorization from a neutral magistrate. Importantly, Clearview AI didn’t just link to Smith’s personal blog, it linked to a story published about him published by his alma mater’s alumni magazine, his profile page from an online group, and a URL of his Facebook page, including the names of people with connections to him, like a faculty advisor and family member.\(^\text{228}\) Should the police have access to all this information without a warrant? This should be a resounding “no” because otherwise, allowing the police unchecked access to such a powerful tool is to put “the liberty of every man in the hands of every petty officer.”\(^\text{229}\)

\(^{227}\) See discussion supra Section I.B.i.

\(^{228}\) See discussion supra Section I.B.i.

\(^{229}\) Boyd v. United States, 116 U.S. 616, 625 (1886).