AMAZON’S NEIGHBORHOOD WATCH

Jackson Eskay*

DoorBot, a technology startup, featured on the fifth season of NBC’s hit entrepreneurial reality show, Shark Tank. It offered customers the ability to see, hear, and speak to anyone at their front door with its single product, the “video doorbell.” After the product pitch, Robert Herjavec, one of the investor-sharks, said “it freaks me out.” DoorBot did not secure a deal.

In 2014, the company rebranded to Ring—a double entendre capturing meaning from both the doorbell’s “ring” and the “ring” of security provided around the home. It also inaugurated its mission statement: “[M]ake neighborhoods safer.” In 2018, Amazon acquired Ring for a deal valued at more than $1 billion. More than 2,000 partnerships now exist between Amazon’s Ring (“Ring”) and law enforcement agencies across the United

* J.D., University of Pennsylvania Carey Law School, 2022. Thank you to Professor Michael Levy for inspiring this Comment. Thank you to Professor David Rudovsky for the mentorship. Thank you to everyone at the University of Pennsylvania Journal of Constitutional Law for the time spent editing and providing feedback. This Comment is dedicated to my late grandfather, Buck, who told me to keep writing, and my grandmother, Dear, who reviewed every draft, from idea to publication.

1 Shark Tank: Season 5, Episode 9 (NBC television broadcast Nov. 13, 2013).
2 Id.
3 Id.
4 Id.
These partnerships streamline government access to video recorded from privately owned devices. More than three million Ring cameras are online nationwide. This is the “The New Neighborhood Watch.”

Ring’s partnerships with law enforcement pose important questions about the role of private companies in government surveillance. The united effort presents a novel surveillance scheme amid an explosion of surveillance technologies and systems implemented by both the private sector and the government. Ring is rapidly increasing its number of partnerships with law enforcement, developing more intimate relationships with individual agencies, and growing its total number of cameras, and

9 BARRY FRIEDMAN, FARHANG HEYDARI, MAX ISAACS & JULIAN CLARK, RING NEIGHBORS & NEIGHBORS PUBLIC SAFETY SERVICE: A CIVIL RIGHTS & CIVIL LIBERTIES AUDIT 4 (2021), https://static1.squarespace.com/static/38a33e881b631be60d4d8b31/t/61a9a9f6e4c4282092bdf7c3/1639623534675/Policing+Project+Ring+Civil+Rights+Audit+%28Full%29.pdf [https://perma.cc/QU6X-74B6].


13 Harwell, Home-Security Cameras, supra note 11 (“Ring stands alone among the tech giants willing to help police get customers’ home video.”).


16 Harwell, supra note 11 (“More than 2,000 police and fire departments across the U.S. have cooperative agreements with Ring system, up from 60 in 2018, a Washington Post analysis of company data shows. The pace of new sign-ups has rapidly accelerated, to two new ‘partnerships’ a day.”).

17 See infra pp. 16–18.

18 Harwell, Home-Security Cameras, supra note 11 (“Dan Calacci, a researcher at the Massachusetts Institute of Technology’s Media Lab who has analyzed usage of Ring’s Neighbors app, estimated that more than 3 million Ring cameras are now online nationwide.”).
innovating for more powerful technology. Privacy advocates around the country are calling for reform.

This Comment explores the Fourth Amendment questions raised by the partnerships between Ring and law enforcement. The Fourth Amendment protects the right to be free from “unreasonable searches and seizures.” It safeguards “reasonable expectations of privacy” by providing “obstacles in the way of a too permeating police surveillance.” Typically, courts evaluate government surveillance through the lens of the Fourth Amendment. This Comment adopts that same approach and argues that law enforcement should be required to obtain a warrant before requesting video footage from Ring’s camera network.

Part I of this Comment charts the Supreme Court’s evolving Fourth Amendment case law and outlines the modern framework for the Fourth Amendment’s warrant requirement. Part II provides factual background about Ring, its flagship product (the Video Doorbell), its virtual network (the Neighbors app), and its partnerships with law enforcement. Part III

---

19 Id. (“Ring said last week that its newest model boasts radar sensors that can track a person’s movement, upgraded cameras that can record visitors from ‘head to toe,’ and improved ‘3D Motion Detection’ that can spot someone from up to 30 feet away. The company has also advertised an unreleased camera drone, the Always Home Cam, that could fly itself around indoors.”); Peter Holley, This Patent Shows Amazon May Seek to Create a Database of Suspicious Persons’ Using Facial-Recognition Technology, WASH. POST (Dec. 18, 2018, 4:01 PM), https://www.washingtonpost.com/technology/2018/12/13/this-patent-shows-amazon-may- seek-create-database-suspicious-persons-using-facial-recognition-technology/ [https://perma.cc/LCK4-TTXV].


21 U.S. CONST. amend. IV.


26 Nick, supra note 12.
applies the Fourth Amendment framework to the questions presented by Ring’s partnerships with law enforcement. It discusses three long-established doctrines (the “public view doctrine,” the “third-party doctrine,” and the doctrine of Fourth Amendment standing) and several federal cases that involve analogous surveillance technology and techniques. Part IV briefly considers model legislation proposed by the ACLU that offers communities more transparency into law enforcement’s surveillance practices. Part V concludes: The Fourth Amendment’s modern privacy-and-technology-conscious jurisprudence recommends restraining Amazon’s New Neighborhood Watch. Law enforcement must obtain a warrant before requesting Ring footage.

I. THE FOURTH AMENDMENT

The Fourth Amendment “erects a wall between a free society and overzealous police action—a line of defense implemented by the framers to protect individuals from the tyranny of the police state.”27 It states in full:

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.28

In more general and discrete terms, it protects against “unreasonable searches and seizures”, and it does so with a “[w]arrant” requirement that conditions any such intrusions on “probable cause” and “particular[ity].”29 A “search,” for purposes of the Fourth Amendment, can occur in two situations: (1) the government physically trespasses on to persons, houses, papers, or effects with intent to obtain information;30 or (2) the government violates a person’s subjective expectation of privacy that society recognizes as reasonable.31 This respectively covers the property interest and the privacy

28 U.S. CONST. amend. IV.
29 Id.
interest secured by the Fourth Amendment. In either situation (and they often overlap) a government search is unlawful unless authorized by a valid warrant (or if an exception to the warrant requirement applies). The warrant requirement places the judgment of an independent magistrate between law enforcement and citizens’ interests in property and privacy. It conditions any invasion of those interests upon a showing of probable cause, and it limits that invasion by specification of the place that will be searched and the evidence desired.

The Supreme Court described and defined Fourth Amendment protection exclusively in terms of property rights until the latter half of the twentieth century. In Boyd v. United States (1886), the Court struck down a statute requiring a person to produce private papers to the government. In the majority opinion, the Court outlined a hierarchy of personal property rights and authorized a search only if the government had a superior interest (compared to the citizen) in the item or place to be searched. Under this theory, the Fourth Amendment requires the government to obtain a search warrant whenever it interferes with a property right.

The Court reinforced this idea in Olmstead v. United States (1928). Roy Olmstead and several other defendants were convicted of a conspiracy to

---

32 See Stefan Ducich, These Walls Can Talk! Securing Digital Privacy in the Smart Home Under the Fourth Amendment, 16 DUKE L. & TECH. REV. 278, 284–85 (2018) ("Supreme Court jurisprudence . . . has vacillated between a purely property (in rem) conception, to one based on expectations of privacy (in personam), to a hybrid of the two.") (footnotes omitted).
33 The most important exceptions are (1) search incident to arrest; (2) exigent circumstances; (3) consent; (4) border searches; and (5) government workplace computers. ORIN KERR, COMPUTER CRIME LAW 454 (4th ed. 2018).
34 U.S. CONST. amend. IV.
35 See Brinegar v. United States, 338 U.S. 160, 175–76 (1949) ("Probable cause exists where the facts and circumstances within their [the officers’] knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed.") (alterations in original) (internal citations and quotations omitted).
36 See Marron v. United States, 275 U.S. 192, 196 (1927) ("The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.").
37 See Ducich, supra note 32, at 285.
38 116 U.S. 616 (1886).
39 Id. at 641.
40 Id. at 623.
41 277 U.S. 438 (1928).
import alcohol during Prohibition. The government tapped the phones of the defendants’ houses and listened to their conversations to obtain evidence for the conviction. The Court held that the Fourth Amendment did not regulate telephone wiretapping. Relying on a trespass theory of property rights, the Court reasoned that because the wires were physically located in public spaces no “trespass upon any property of the defendants” occurred. The government therefore did not violate the Fourth Amendment because it did not need to obtain a warrant.

Under the Boyd-Olmstead framework, Fourth Amendment cases consistently turned on the determination of whether the government entered protected property without a warrant. The Court abrogated this property-based theory in 1967, when it decided Katz v. United States. In Katz, the FBI, acting without a warrant, attached an electronic listening and recording device on the outside of a public phone booth. The Court held that this violated the Fourth Amendment. Writing for the majority, Justice Stewart reasoned that “the Fourth Amendment protects people, not places,” and he rejected the idea that its protections “turn upon the presence or absence of a physical intrusion into any given enclosure.”

Katz declared privacy, not property, as the fundamental interest upon which Fourth Amendment rights were premised. In his concurring opinion, Justice Harlan introduced the idea of a “reasonable expectation of privacy,” which has been central to the enduring legacy of Katz in Fourth Amendment jurisprudence.

---

42 Id. at 455.
43 Id. at 466.
44 Id. at 466.
45 Id. at 457.
46 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.”).
49 Id. at 348.
50 Id. at 359.
51 Id. at 351.
52 Id. at 353.
53 Id. at 351 (“[T]he Fourth Amendment protects people, not places.”).
Amendment jurisprudence. As Harlan described, this is the notion that the Fourth Amendment protects a person’s subjective expectation of privacy that society recognizes as objectively reasonable.

The Court almost exclusively used this “reasonable expectation of privacy” test to determine the scope of Fourth Amendment protections until it decided United States v. Jones (2012). In Jones, Antoine Jones was suspected of being involved in a large-scale drug trafficking operation. The FBI, again, acting without a warrant, placed a GPS tracking device on Jones’s vehicle and used the device to track his movements for twenty-eight days, collecting an upwards of 2,000 pages of data. The Court held that the government acted unlawfully by installing a GPS tracking device on Jones’s vehicle without a warrant. Writing for the majority, Justice Scalia reasoned that the Fourth Amendment “must provide at a minimum the degree of protection it afforded when it was adopted,” and this meant preserving the property-based theory. Accordingly, both the property interest and the privacy interest are essential to a Fourth Amendment inquiry, and neither serves as “the exclusive test.” In this case, the trespass on Jones’s vehicle was determinative, however, so the Court did not reach the Katz privacy analysis.

Justice Sotomayor concurred in the judgment but wrote separately to reemphasize that “the Fourth Amendment is not concerned only with trespassory intrusions of property.” She recognized that GPS surveillance reveals “a wealth of detail about [a person’s] familial, political, professional, religious, and sexual associations,” and “[a]wareness that the government

---

54 Id. at 360 (Harlan, J., concurring).
55 Id. at 361 (Harlan, J., concurring) (“[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’

56 565 U.S. 400 (2012); see Ducich, supra note 32, at 289 (noting “the Court’s exclusive reliance on expectations of privacy since Katz . . . .

57 Jones, 565 U.S. at 402.
58 Id. at 402–03.
59 Id. at 413 (affirming the lower court’s decision).
60 Id. at 411.
61 Id.
62 Id.
63 Id. at 413.
64 Id.
65 Id. at 415 (Sotomayor, J., concurring).
may be watching chills [these] associational and expressive freedoms.”

She argued that Fourth Amendment analysis must consider these attributes of GPS monitoring to determine whether a reasonable expectation of privacy exists.

Justice Alito, in his concurring opinion, rejected the property-based trespass theory altogether, calling it “unwise” and “highly artificial.” Alito criticized the majority for focusing on the relatively innocuous trespass instead of the more significant GPS monitoring. He argued that “current Fourth Amendment case law” necessitated the reasonable-expectation-of-privacy test inaugurated in Katz. Under this test, he suggested that “the long-term [GPS] monitoring of [Jones’] movements” constituted a Fourth Amendment violation. Alito acknowledged the many difficulties in applying the Katz test—including how technology alters individual and societal expectations of privacy—but still maintained it was the best method available to the Court to analyze Fourth Amendment claims. In light of these difficulties, he wrote that “[a] legislative body is [better] situated to gauge changing public attitudes, . . . draw detailed lines, and . . . balance privacy and public safety in a comprehensive way.”

The decision in Jones left open many questions about how Fourth Amendment protections extend in the advent of new technology. The Court grappled with some of these issues in Riley v. California (2014) and Carpenter v. United States (2018).

In Riley, a police officer stopped David Riley for a traffic violation, which eventually lead to his arrest for weapons charges. The officer searching Riley, incident to the arrest, seized his smart phone without a warrant; as a result of this search, Riley was linked by law enforcement to a gang

---

66 Id. at 416 (Sotomayor, J., concurring).
67 Id. (Sotomayor, J., concurring).
68 Id. at 419 (Alito, J., concurring).
69 Id. at 423–25 (Alito, J., concurring).
70 Id. at 419 (Alito, J., concurring).
71 Id. at 427 (Alito, J., concurring).
72 Id. at 430 (Alito, J., concurring).
73 Id. at 429–30 (Alito, J., concurring).
74 See id. at 427 (Alito, J., concurring) (discussing how changes in technology might shape Fourth Amendment analysis).
75 573 U.S. 373 (2014).
shooting.\textsuperscript{78} The “search incident to arrest” rule is an exception to the warrant requirement that allows an officer to search an arrestee and any item or areas within his immediate reach and control at the time of a lawful arrest.\textsuperscript{79} The question for the Court in\textsuperscript{Riley} was whether this exception, which has been applied to things like wallets and purses, also extends to smart phones.\textsuperscript{80} The Court held that it does not.\textsuperscript{81} In the unanimous majority opinion, Chief Justice Roberts argued that smart phones “differ in both a quantitative and a qualitative sense” from other objects covered by the exemption.\textsuperscript{82} For example, smart phones contain the contents of call logs, text messages, e-mails, internet browsing history, calendars, photographs, videos, books, music, journal entries, and more.\textsuperscript{83} This centralized trove of information, and all that it may reveal, holds “the privacies of life” for many Americans.\textsuperscript{84}

Based on these features, the Court held that a warrant must be obtained before searching a smart phone seized “incident to an arrest.”\textsuperscript{85} Justice Alito, in his concurring opinion, again called for “legislation that draws reasonable distinctions based on categories of information or . . . other variables.”\textsuperscript{86} Similar to his concurrence in\textsuperscript{Jones}, he noted that legislatures are better equipped to respond to technological changes affecting privacy than “the blunt instrument of the Fourth Amendment.”\textsuperscript{87}

In\textsuperscript{Carpenter}, police arrested four men in connection with a series of armed robberies.\textsuperscript{88} One of the men confessed to the crime and provided his cell phone number and the numbers of other participants.\textsuperscript{89} Cell phones and other wireless devices connect to cell towers several times a minute, creating a detailed record of the device’s approximate location, known as historical

\textsuperscript{78} Id.
\textsuperscript{79} Id. at 383.
\textsuperscript{80} Id. at 393 (“[I]nspecting the contents of an arrestee’s pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.”)
\textsuperscript{81} Id. at 403.
\textsuperscript{82} Id. at 393.
\textsuperscript{83} Id.
\textsuperscript{84} Id. at 403 (internal quotation marks and citation omitted).
\textsuperscript{85} Id.
\textsuperscript{86} Id. at 408 (Alito, J., concurring).
\textsuperscript{87} Id. (Alito, J., concurring).
\textsuperscript{89} Id.
cell-site location information (CSLI). The FBI obtained historical CSLI from the wireless carriers of these numbers without a warrant, and based on this evidence, charged Timothy Carpenter with robbery, among other offenses.

The government argued that “the third-party doctrine” allowed for the warrantless acquisition of historical CSLI. This is “the notion that an individual has a reduced expectation of privacy in information knowingly shared with another.” For example, business records “possessed, owned, and controlled” by a third party, such as a credit card statement, can typically be obtained without a warrant. The government argued that because CSLI is shared with wireless carriers it is not protected by the Fourth Amendment. The Court disagreed.

Writing for the majority, Justice Roberts noted that “diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely.” He argued that a person maintains a “reasonable expectation of privacy in the whole of his physical movements,” and that a “world of difference” exists between the information contained in historical CSLI compared to other business records exempted by the third-party doctrine. Historical CSLI, for example, offers “near perfect surveillance” that “runs against everyone.” Without the protection of the warrant, the government would have unfettered access to the precise movements of everyone owning a cell phone. The Court kept a narrow holding, not bearing on “other business records . . . . [or] collection techniques,” but also acknowledged its responsibility to “contend with the seismic shifts in digital technology” when answering Fourth Amendment questions.

***

90 Id. at 2211.
91 Id. at 2212.
92 Id. at 2219. This doctrine is discussed in more detail in Part III.
93 Id. at 2219.
94 Id. at 2223–24 (Kennedy, J., dissenting).
95 Id. at 2219.
96 Id. at 2223.
97 Id. at 2219 (citing Riley v. California, 473 U.S. 373, 392 (2014)).
98 Id. at 2219.
99 Id. at 2218.
100 Id.
101 Id. at 2220.
102 Id. at 2219.
Katz, Jones, Riley, and Carpenter supply the modern framework for Fourth Amendment analysis. In this framework, Fourth Amendment questions must contend with how the advent of new technology affects both a person’s property interest and his reasonable expectation of privacy. The concurring opinions in Jones, and the recent decisions in Riley and Carpenter, demonstrate that “digital is different.”

II. The New Neighborhood Watch

Few companies in the world are as established as Amazon. Amazon is a multinational technology company based in Seattle, Washington, focusing on e-commerce, cloud computing, digital streaming, and artificial intelligence. It is widely recognized as “one of the most influential economic and cultural forces in the world.”

As the largest e-commerce retailer in the United States, Amazon ships more than 2.5 billion packages each year. This delivery volume, however, makes it vulnerable to a growing problem: Around the country, more than 1.7 million packages are lost or stolen each day, adding up to more than $25

---

104 See Andrew Guthrie Ferguson, Future-Proofing the Fourth Amendment, HARV. L. REV. BLOG (June 25, 2018), https://blog.harvardlawreview.org/future-proofing-the-fourth-amendment/ [https://perma.cc/LX9N-GL67] (explaining that the Carpenter opinion “institutionalizes the ‘digital is different’ theme [that was] initiated in Riley v. California”).
million in daily losses. In New York City alone, more than 90,000 packages disappear daily. Most Amazon deliveries arrive without an issue, but it typically replaces or reimburses any stolen products, giving it a strong financial incentive to reduce the number of thefts. This incentive helps explain its acquisition of Ring and interest in assisting law enforcement. Amazon is creating a new platform for policing.

A. Amazon’s Ring and Its Police Partnerships

Ring, a wholly owned subsidiary of Amazon, offers a slate of home-security products. The Video Doorbell, its flagship product, mounts on a home’s doorbell, connects to the Wi-Fi Network, and then sends alerts to a connected smart phone app when it detects motion or when someone presses the doorbell. Customers can then see, hear, and speak to visitors from anywhere. The baseline model includes 1080p High-Definition Video, two-way audio, advanced motion detection, night vision, and “Live View”

109 Id.
110 See id. (“[O]nline retailers typically refund or replace items for free, often with few questions.”).
113 Jeffrey Dastin & Greg Roumeliotis, Amazon Buys Startup Ring in $1 Billion Deal to Run Your Home Security, REUTERS (Feb. 27, 2018, 4:05 PM), https://www.reuters.com/article/us-ring-m-amazon-com/amazon-buys-startup-ring-in-1-billion-deal-to-run-your-home-security-idUSKCN1GB2VG [https://perma.cc/J7PM-BPMQ] (“Ring’s security devices could work well with Amazon Key, a smart lock and camera system that lets delivery personnel put packages inside a home to avoid theft or, in the case of fresh food, spoiling.”).
(which streams real-time video at the tap of a button).\textsuperscript{119} Videos can be saved and shared in the app;\textsuperscript{120} and features can be customized according to user preference—for example, the alerts for motion detection can be limited to specific areas.\textsuperscript{121} The camera provides a detailed view from the front-door, but it also captures high-resolution images of “homes across the street and down the block.”\textsuperscript{122} Ring provides free cloud storage for sixty days but then asks customer to enroll in its Ring’s “Basic Protect Plan.”\textsuperscript{123} It also offers the “Pro Protect Plan,” which includes “24/7 professional monitoring.”\textsuperscript{124} After the sixty days, Ring customers can save videos and images only if they purchase a cloud services plan.\textsuperscript{125}

After installing a product, Ring encourages customers to download “Neighbors,” its community-based social app.\textsuperscript{126} The app provides a platform for customers to share information and content related to crime and safety with the people in their community.\textsuperscript{127} Users are anonymous on the app, but the faces and voices they capture on video and post publicly are neither censored nor obscured.\textsuperscript{128}

Utilizing this model—that connects private-surveillance products to a community social app—Ring secured more than 2,000 partnerships with law enforcement agencies across the United States.\textsuperscript{129} Montana and Wyoming

\textsuperscript{119} Id.
\textsuperscript{120} Id.
\textsuperscript{121} Id.
\textsuperscript{124} Id.
\textsuperscript{125} Id.
\textsuperscript{128} Harwell, Doorbell-Camera Ring Firm, supra note 122.
\textsuperscript{129} Harwell, Home-Security Cameras, supra note 1); BARRY FRIEDMAN, FARHANG HEYDARI, MAX ISAACS & JULIAN CLARK, RING NEIGHBORS & NEIGHBORS PUBLIC SAFETY SERVICE: A CIVIL
are the only two states without any partnerships. Ring works aggressively with the government to incentivize sales. It offers discounts to cities and community groups that use funds to purchase Ring products, and it gives free cameras to police departments to distribute to local homeowners. For example, in 2019, the Boca Raton Police Foundation launched a joint subsidy program with Ring, enabling “200 verified City of Boca Raton residents to receive a $100 discount code to use towards the purchase of select Ring security devices.” In a similar move, Ring gave the police department in Lakeland Florida fifteen free security cameras.

As part of its agreements, Ring offers police departments access to the Law Enforcement Neighborhood Portal, a bespoke account to the Neighbors app. Through this portal, law enforcement can view all the public posts made in the Neighbors app within their jurisdiction and chat directly with users on the Neighbors Feed. Moreover, agencies can request video from Ring users to aid in investigating crimes. So far, the mechanism for

---

130 Rights & Civil Liberties Audit 4 (2021), https://static1.squarespace.com/static/58a3e881b631be60df48b31f/1/61baab9c4e282092b547e5/1639623584675/Policing+Project+Ring+Civil+Rights+Audit+supra.pdf [https://perma.cc/QU6X-74B6].

131 Lyons, supra note 20.

132 Dell Cameron, Everything Cops Say About Amazon’s Ring Is Scripted or Approved by Ring, GIZMODO (July 30, 2019, 5:34 PM), https://gizmodo.com/everything-cops-say-about-amazons-ring-is-scripted-or-approved-1836812538 [https://perma.cc/VK2J-AX2J].

133 Harwell, supra note 11.


136 Haskins, supra note 115.


requesting user video has undergone two different iterations. In the first iteration, law enforcement used an interactive map to request unpublished Ring videos within a specified area (up to 0.5 square miles) and time range (up to twelve hours). Ring then sent an email to all users in that area with a message from the police. Ring automatically subscribed its users to receive these requests but reserved for them the ability to opt-out, refuse individual requests, and review their videos before deciding to send.

In June of 2021, after an audit by the Policing Project at NYU School of Law, Ring changed this mechanism for requesting video footage. Now, in the second and current iteration, law enforcement can only request user video through “a new, publicly viewable post category on [the Neighbors app] called Request for Assistance.” Law enforcement agencies make a public post, and Ring users can then choose to submit video footage by clicking the “Tap Here to Help” link located in the post. After a user submits their video, officers have a right to use it indefinitely and for any purpose.

The negotiations between Ring and law enforcement are unique for each partnership, but in general the partnerships conform to a simple principle: police get access to a portal that allows them to view and request private surveillance footage, “and the company gets the promotional muscle of the police.” In this framework, Ring controls police statements made about its service, including one-on-one interactions between police and residents. For example, Ring issued a spreadsheet to the Topeka Police 138 Priest, supra note 137.


140 Id.

141 Cameron, supra note 131.

142 FRIEDMAN, HEYDARI, ISAACS & CLARK, supra note 9, at 46–47.


144 Priest, supra note 137.


146 Haskins, supra note 115.

Department in Kansas with forty-six recommended comments to use in interactions with residents on the Neighbor’s app and social media.\textsuperscript{148} Similarly, the Maywood Police Department in New Jersey received a “Reactive Q&A document,” with sample answers to potential questions from the community, a “Sample Social Media Posts” document, and a “Talking Points” document.\textsuperscript{149} In many instances, police departments copy these templates verbatim in their communications with the public and individuals.\textsuperscript{150}

Ring wins these partnerships by indicating an ability to minimize crime. After a study it conducted with the Los Angeles Police Department in 2016, Ring announced a fifty-five percent reduction in burglaries in seven months in a region of Wilshire Park, compared to surrounding areas.\textsuperscript{151} This reduction occurred with only forty devices installed (i.e., ten percent of homes) in the selected area.\textsuperscript{152}

An analysis from \textit{MIT Technology Review}, however, undermined the strength of this finding.\textsuperscript{153} It revealed (1) that crime actually increased in Wilshire Park in a ten-month period when compared to a similar seven-month period in the previous year;\textsuperscript{154} (2) that Ring elected not to publish another study it conducted in a neighboring community (suggesting selective reporting);\textsuperscript{155} and (3) that the only independent study (i.e., not sponsored by Ring) found that neighborhoods with Video Doorbells were actually more likely to suffer break-ins than those without them.\textsuperscript{156}

This lack of strong evidence has not discouraged police departments from forming these partnerships, however, and the partnerships continue to grow more intimate and intentional. In 2019, Amazon arranged a sting operation
with the police department in Aurora, Colorado, to apprehend package thieves in the area.\textsuperscript{157} Amazon sent twenty-five boxes with GPS trackers to be placed at homes with Ring devices installed.\textsuperscript{158} They also provided fifteen Ring Video Doorbells in case residents did not have a device installed or preferred to use a donated device.\textsuperscript{159} The operation did not result in a single arrest or even a package thief caught on camera.\textsuperscript{160} Still, the Public Relations Coordinator for Ring assured that the “community will appreciate that Aurora PD is being so proactive . . . .”\textsuperscript{161}

In Bloomfield, New Jersey, the Detective Bureau Commander asked a Ring representative how the police department could encourage more people to submit Ring camera footage.\textsuperscript{162} In an email, he wrote: “I have been requesting videos but have not been getting any responses . . . [Is] there anything that we can blast out to encourage Ring owners to share the videos when requested?”\textsuperscript{163} The Ring representative advised pairing all video requests through the Law Enforcement Neighborhood Portal with a public post on the Neighbors app and provided an example post.\textsuperscript{164} The representative also recommended posting often and consistently on the Neighbors app, as this tends to lead to higher opt-in rates from the community.\textsuperscript{165}

In Bexar County, Texas, Ring donated cameras to the County Sheriff’s Office in exchange for promoting the Neighbors app. A ring representative explained in an email, “[t]he more people on the [Neighbors] app the more valuable the platform becomes for your agency AND [sic] Ring will donate

\begin{flushleft}
\end{flushleft}

\begin{flushleft}
\textsuperscript{158} Id.
\end{flushleft}

\begin{flushleft}
\textsuperscript{159} Id.
\end{flushleft}

\begin{flushleft}
\textsuperscript{160} Id.
\end{flushleft}

\begin{flushleft}
\textsuperscript{161} Id.
\end{flushleft}

\begin{flushleft}
\end{flushleft}

\begin{flushleft}
\textsuperscript{163} Id.
\end{flushleft}

\begin{flushleft}
\textsuperscript{164} Id.
\end{flushleft}

\begin{flushleft}
\textsuperscript{165} Id.
\end{flushleft}
a camera to the Bexar County community for every twenty downloads.”

The Sheriff’s Office earned fifteen “donation devices” for facilitating 279 app downloads from Bexar County residents (which Ring rounded up to 300).

***

Sales for Ring devices continue to increase rapidly. As part of its marketing strategy, Ring shares and promotes videos of user-generated content—recordings of averted criminal activity, interactions with delivery persons, candid moments with family and friends, and curious animals around the home. Ring wins its customers by giving them the impression of increased safety, coupled with the convenience and intrigue of having a video feed at the front door. What Ring does not mention, however, are the neighbors across the street or down the block—those people ultimately subject to the video recordings police can request—that it enrolls in this surveillance system automatically, without consent, and without a mechanism to opt-out.

Amazon’s policing platform (1) incorporates citizen-owned security cameras (the Ring Video Doorbell) that it (2) configures in a virtual network (the Neighbors app) and (3) streamlines for government access (the Law Enforcement Neighborhood Portal). This design allows law enforcement to access a network of surveillance footage without a warrant. Hereinafter, this surveillance system will be referred to as the New Neighborhood Watch or the “NNW.”

As detailed above in Part I, the Supreme Court’s most recent and important cases reveal a trend away from mechanical interpretation and application of the Fourth Amendment and instead advocate a technology-conscious jurisprudence that accounts for the power of new surveillance technology.

---


167 Id.


170 Id.

171 See supra pp. 12–18.
This trend suggests that law enforcement requests for Ring video footage through the Law Enforcement Neighborhood Portal should require a warrant.

The next section addresses the Fourth Amendment questions posed by the NNW. It examines three long-standing doctrines and several federal cases to make the argument that law enforcement should be required to obtain a warrant before requesting Ring video footage.

III. THE FOURTH AMENDMENT AND THE NEW NEIGHBORHOOD WATCH

The primary Fourth Amendment question presented by the NNW is whether law enforcement’s requests for Ring footage should require a warrant. In answering this question, this section discusses three long-established Fourth Amendment doctrines—“the public view doctrine,” the “third-party doctrine,” and the doctrine of Fourth Amendment standing—in addition to several federal cases ruling on analogous surveillance technology and techniques. These three doctrines and the relevant federal cases are discussed below.

A. Fourth Amendment Doctrines

The Supreme Court’s decision in *Katz* marked a seminal shift in Fourth Amendment jurisprudence by introducing a privacy interest in addition to the long-established property interest. The expectation-of-privacy-test created a legal mechanism flexible enough to contend with emerging surveillance technologies and systems. Following *Katz*, however, several doctrines emerged that narrowed privacy considerations, putting many

---

172 See Ferguson, supra note 104 (“Signaling a new openness to expand the Fourth Amendment to fit digital criminal investigations, the Carpenter majority resisted a ‘mechanical interpretation’ of the Fourth Amendment’ insisting that the ‘new,’ ‘novel,’ ‘unique,’ ‘seismic’ change in technologies warrants a different outcome. This recognition of digital transformation signals a new openness to ensure that the Fourth Amendment protects the digital lives of citizens.”) (citing United States v. Carpenter, 138 S. Ct. 2206 (2018)).

173 Daniel T. Pesciotta, *I'm Not Dead Yet: Katz, Jones, and the Fourth Amendment in the 21st Century*, 63 CASE W. RESERVE L. REV 187, 188 (2012). (“[E]ver since the Court’s seminal ruling in *Katz v. United States*, the Court as held that warrantless searches that encroach upon a citizen’s reasonable expectation of privacy are unconstitutional.”).

contemporary surveillance techniques beyond the reach of the Fourth Amendment.\textsuperscript{175}

1. The Public View Doctrine

The \textit{Katz} Court explained that “\textit{w}hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.”\textsuperscript{176} Given the facts of the case, this meant that while Katz could reasonably expect his telephone conversation to be private, he could not expect the same of his movements inside the telephone booth, which were visible to the public: “[W]hat he sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear.”\textsuperscript{177} Following this logic, the public view doctrine developed in subsequent cases to hold that law enforcement is entitled to make observations from any lawful vantage point (i.e., any vantage point available to the public) without the need to first secure a warrant.\textsuperscript{178} Consider two prominent examples.

In \textit{California v. Ciraolo} (1986),\textsuperscript{179} police officers received an anonymous tip that Dante Ciraolo was growing marijuana in his backyard, which he enclosed with a ten-foot fence.\textsuperscript{180} The investigating officer secured a private plane and, without a warrant, flew over Ciraolo’s house at an altitude of 1,000 feet.\textsuperscript{181} From the air, he identified marijuana plants growing.\textsuperscript{182} The Court held that this did not constitute a search, stating that “[t]he 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.”\textsuperscript{183}

The Court was presented with a very similar set of facts in \textit{Florida v. Riley} (1989).\textsuperscript{184} Law enforcement, acting without a warrant, circled Michael

\textsuperscript{175} Id.
\textsuperscript{176} \textit{Katz}, 398 U.S. at 351.
\textsuperscript{177} Id. at 352.
\textsuperscript{178} See \textit{Florida v. Riley}, 488 U.S. 445, 449 (2018) (“As a general proposition, the police may see what may be seen ‘from a public vantage point where [they have] a right to be.’”) (citing \textit{California v. Ciraolo}, 476 U.S. 207, 213 (1986)).
\textsuperscript{179} 476 U.S. 207 (1986).
\textsuperscript{180} Id. at 209.
\textsuperscript{181} Id.
\textsuperscript{182} Id.
\textsuperscript{183} Id. at 215.
Riley’s property with a helicopter at an altitude of 400 feet in order to confirm an anonymous tip that he was growing marijuana. The Court held that this did not constitute a search because “the police officer did no more” than “[a]ny member of the public [that] could legally have been flying over Riley’s property . . . .”

These two cases help illuminate the scope of the public view doctrine. But determining what a person “knowingly exposes to the public” is not always straightforward, especially in the event of persistent surveillance. The Supreme Court recognized these challenges in Jones and Carpenter. A majority of justices in the Jones opinion expressed deep concern about long-term GPS monitoring that reveals a person’s physical movements in their entirety. The Court in Carpenter found that government access to historical CSLI “contravenes [the] expectation” that law enforcement will not “secretly monitor and catalogue every single movement of an individual[].” GPS monitoring and CSLI both track movement that is publicly observable, but the Court nonetheless made resolute: “A person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, ‘what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.’”

In its Guidelines for Public Video Surveillance, The Constitution Project, a non-profit devoted to government oversight, describes the notions of privacy imperiled by an overreaching public view doctrine:

Most people expect to remain anonymous in many “public” contexts, such as entering an Alcoholics Anonymous meeting, a psychiatrist’s office, an infertility clinic, or the headquarters of a fringe religious or cultural group. Similarly, even when they are in a public place, most people expect to keep private the information that might be detectable from such sources as the exposed words on a vial of prescription drugs, the moving lips of a couple...
engaged in hushed conversation, or diary entries written by a person sitting on a park bench.\textsuperscript{191}

The NNW jeopardizes these notions of privacy. The Los Angeles Police Department, for example, requested footage of Black Lives Matter protests from Ring users in 2020.\textsuperscript{192} Emails sent on behalf of the “Safe L.A. Task Force” asked specifically “for footage related to the recent protests.”\textsuperscript{193} The opinions in Jones and Carpenter indicate that Fourth Amendment analysis should consider such broad and indiscriminate surveillance capability because it risks “chill[ing] associational and expressive freedoms.”\textsuperscript{194}

The NNW’s surveillance power emerges from its network of cameras. Cameras fundamentally augment a person’s observational ability by allowing them to see things more than once or to see things otherwise inappreciable or imperceptible. For example, cameras developed at MIT capture the vibrations of sound, turning silent video into audio recordings;\textsuperscript{195} casinos use cameras that can read text messages on a phone;\textsuperscript{196} and Boston Logan Airport installed a camera that can see any object more than one-and-a-half centimeters wide within 150 meters.\textsuperscript{197} Ring cameras are not yet this powerful,\textsuperscript{198} but, in 2018, Amazon filed a patent application indicating an interest to eventually augment Ring cameras with its facial recognition

\begin{itemize}
  \item \textsuperscript{192} Mathew Guariglia & Dave Maass, LAPD Requested Ring Footage of Black Lives Matter Protests, ELEC. FRONTIER FOUND. (Feb. 16, 2021), https://www.eff.org/deeplinks/2021/02/lapd-requested-ring- footage-black-lives-matter-protests [https://perma.cc/C2SB-GQRM].
  \item \textsuperscript{193} Id. Ring footage requests typically require a case number, but when asked, “[the LAPD] would not cite a specific crime they were investigating.” Id.
  \item \textsuperscript{194} United States v. Jones, 565 U.S. 400 416 (2012); Carpenter, 138 S.Ct at 2217.
  \item \textsuperscript{196} Lori Culbert, Judge Raps Police for Using Casino Cameras to Read Suspect’s Texts, VANCOUVER SUN [Nov. 11, 2014], https://vancouversun.com/News/judge-raps-police-for-using-casino-cameras-to-read-suspects-texts/wcm/91550ff2-87cb-4c34-aab3-da05aca0098 [https://perma.cc/XEG3-LS8B].
  \item \textsuperscript{197} Brian R. Ballou, At Logan, New Device Keeps Eye on Everything, BOS. GLOBE (May 3, 2010), http://archive.boston.com/news/local/massachusetts/articles/2010/05/03/at_logan_new_device_keeps_eye_on_everything/ [https://perma.cc/58EC-6YPU].
  \item \textsuperscript{198} Video Doorbell, RING.COM: PRODUCTS, https://ring.com/collections/all-products/products/video- doorbell/v2 [https://perma.cc/9FQ8-W2HT] [last visited Apr. 7, 2020].
\end{itemize}
technology,\textsuperscript{199} Rekognition.\textsuperscript{200} The technology can ascertain a person’s emotional expression\textsuperscript{201} and would be used to develop a “database of suspicious persons.”\textsuperscript{202}

Advanced camera systems therefore change the dynamic central to the public view doctrine: what is visible to a camera is different (and increasingly so) from “what is visible to the naked eye.”\textsuperscript{203} A camera provides video content that is more “deeply revealing”\textsuperscript{204} and gives “access to a category of information otherwise unknowable.”\textsuperscript{205} These qualities were critical to the decision in \textit{Carpenter} requiring a warrant for government acquisition of historical CSLI.\textsuperscript{206}

Following \textit{Carpenter}, the public view doctrine should not preclude Ring footage from Fourth Amendment protection. Ring footage contains equally, if not more, sensitive information than historical CSLI. Cell-phone tracking is (at least, for the moment) more comprehensive, but video content is more intimately revealing. CSLI informs when a person is home—a simple dot on a map.\textsuperscript{207} But Ring footage shows when that same person is working in the front yard shirtless or enjoying a nightcap on the porch.

To understand the point, consider the opening scene in the acclaimed Pixar film, \textit{Up}.\textsuperscript{208} Critics have described the opening scene as a “masterclass...

\textsuperscript{199} Holley, supra note 19.
\textsuperscript{202} Holley, supra note 19.
\textsuperscript{204} Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).
\textsuperscript{205} Id. at 2218.
\textsuperscript{206} Id.
\textsuperscript{208} UP (Pixar 2009).
in narrative exposition. In less than ten minutes, it tells a complete love story—passion, hope, heartbreak, grief, the whole thing. Many of the shots in the sequence simply depict the exterior of the main character’s home: the mailbox, the driveway, the front-yard, the view from across the street—all images that a Ring Video Doorbell would capture. Content that can compose a narrative of this force should not be excluded from Fourth Amendment protection simply because it is publicly observable.

2. The Third-Party Doctrine

The third-party doctrine (described briefly above in the description of Carpenter) is conceptually very similar to the public view doctrine, but deals with third parties, not the public at large. For a classic example, consider you are planning to rob a bank. You invite your friend Joe to your apartment and, behind closed doors, with no one else around, you inform him of your plans and ask for his assistance. The next day Joe rats to law enforcement. Clearly, this information was not exposed to the public, but nonetheless, because it was shared with a third-party, it is not a subject of Fourth Amendment protection. The third-party doctrine is the rule “that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” Law enforcement can therefore use this information without obtaining a warrant.

In the digital age, where people easily and increasingly share personal information, the third-party doctrine provides the government with a powerful investigative tool. In two of the most prominent third-party

210 Id.
211 Harwell, Doorbell-Camera Ring Firm, supra note 122.
212 See Orin S. Kerr, The Case for the Third Party Doctrine, 107 MICH. L. REV. 561, 563 (2009) (“The rule is simple . . . . a person cannot have a reasonable expectation of privacy in information disclosed to a third party.”).
214 Kerr, supra note 213, at 562 (“[T]he human impulse to share creates an important opportunity for criminal investigators.”).
cases, *United States v. Miller* (1976)\(^{216}\) and *Smith v. Maryland* (1979),\(^ {217}\) the Supreme Court held that acquiring bank records and telephone records, respectively, were not Fourth Amendment searches requiring warrants.\(^ {218}\)

In *Miller*, agents of the Treasury Department’s Alcohol, Tobacco, and Firearms Bureau investigated Mitch Miller for his participation in an illegal whiskey distillery.\(^ {219}\) The agents subpoenaed the presidents of several banks in which Miller had an account to produce all records of his banking history.\(^ {220}\) The Court held that subpoenaing the bank records without a warrant did not violate the Fourth Amendment.\(^ {221}\) Writing for the majority, Justice Powell instructed that a bank customer “takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.”\(^ {222}\) Based on this assertion, Miller could have no reasonable expectation of privacy.\(^ {223}\)

In *Smith*, Baltimore police investigated the robbery of a young woman, who gave a description of the assailant and a vehicle observed near the scene of the crime.\(^ {224}\) The police eventually identified Michael Smith as matching the victim’s description and driving an identical vehicle.\(^ {225}\) Upon police request, Smith’s telephone company “installed a pen register\(^ {226}\) at its central office to record the telephone numbers dialed at [his] home.”\(^ {227}\) The police installed the device without a warrant.\(^ {228}\) Through the pen register, they learned that Smith placed a call to the victim’s phone, which ultimately verified Smith as the robber.\(^ {229}\) The Court held that installing a pen register

\(^{217}\) 442 U.S. 735 (1979).
\(^{218}\) See Kerr, supra note 213, at 569–70 (explaining the Supreme Court’s holdings in *Miller* and *Smith*); *Miller*, 425 U.S. at 446; *Smith*, 442 U.S. at 745–46.
\(^{219}\) *Miller*, 425 U.S. at 437.
\(^{220}\) Id.
\(^{221}\) Id. at 446.
\(^{222}\) Id. at 443.
\(^{223}\) Id. at 442–43.
\(^{225}\) Id.
\(^{226}\) A pen register is a device commonly used by law enforcement that records a list of phone numbers contacted by a specific phone. *Pen Register*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/pen_register [https://perma.cc/MZ9P-CRHD] (last visited Apr. 7, 2021).
\(^{227}\) *Smith*, 442 U.S. at 737.
\(^{228}\) Id.
\(^{229}\) Id. at 737–38.
did not require a warrant.\footnote{id at 745–46.} In the majority opinion, Justice Blackmun expressed “doubt that people in general entertain any actual expectation of privacy in the numbers they dial.”\footnote{id at 742.} Even if Smith did harbor a subjective expectation of privacy, “this expectation is not ‘one society is prepared to recognize as ‘reasonable.’”\footnote{id at 743 (citing Katz v. United States, 389 U.S. 347, 361 (1967)).} Smith “voluntarily conveyed” the telephone numbers to the company in the process of making the call.\footnote{Smith, 442 U.S. at 744.}

The Supreme Court’s decision in 
\textit{Carpenter} explicitly limited the third-party doctrine, however, and established CSLI as a category of information deserving Fourth Amendment protection.\footnote{See Carpenter v. United States, 138 S. Ct. 2206, 2219–20 (2018); Susan Freiwald & Stephen Wm. Smith, Comment, \textit{The Carpenter Chronicle: A Near-Perfect Surveillance}, 109 HARV. L. REV. 205, 206 (2018) (“[T]he \textit{Carpenter} Court adopted a normative approach well suited for the question presented [by historical CSLI] . . . [that] significantly circumscribed the ‘third-party doctrine.’”).} First, the Court noted that 
\textit{Smith} and 
\textit{Miller} “did not rely solely on the act of sharing. Instead, they considered ‘the nature of the particular documents sought’ to determine whether ‘there is a legitimate expectation of privacy concerning their contents.’”\footnote{Carpenter, 138 S. Ct. at 2219 (citing United States v. Miller, 425 U.S. 435, 422 (1976)).} In this regard, the Court deemed the privacy concerns relating to historical CSLI legitimate—and markedly more significant than bank or telephone records.\footnote{Carpenter, 138 S. Ct. at 2219 (citing Smith, 442 U.S. at 745).} Second, the Court acknowledged that CSLI is not “truly shared” or “voluntarily conveyed,” but rather, recorded as a “dint of [the cell phone’s] operation, without any affirmative act on the part of the user.”\footnote{Id. at 2219–20.} Therefore, a cell phone user does not, in any meaningful sense, voluntarily “assume the risk” of handing over a “comprehensive dossier of his physical movements.”\footnote{Id. at 2220 (citing Smith, 442 U.S. at 745).}

Following the decision in 
\textit{Carpenter}, the third-party doctrine should not exempt Ring surveillance footage from the warrant requirement. Ring Video Doorbells \textit{capture} footage of neighbors and their homes—in no way do
these persons voluntarily share this content.\textsuperscript{239} This dynamic alone precludes application of the third-party doctrine.\textsuperscript{240} But assuming \emph{arguendo} that a court could say otherwise, Ring footage, as discussed above, contains equally, if not more sensitive information than CSLI.\textsuperscript{241} A “comprehensive dossier of physical movements” displayed using dots on a map implicates serious privacy concerns, but it cannot be used to compose “a masterclass in narrative exposition.” Video content captured by Ring cameras is more personal and penetrating—it reveals facial expression, body language, and discrete movements, in addition to localized geographic information.

3. \textit{Fourth Amendment Standing}

To bring a lawsuit to federal court, a plaintiff must show that he suffered, or is at impending risk of suffering, a specific injury.\textsuperscript{242} This injury (or risk of injury) must be the result of an action by the defendant, and the court must be able to provide some form of remedy.\textsuperscript{243} This “standing” requirement derives from Article III of the Constitution, which governs the judiciary.\textsuperscript{244} In the context of the Fourth Amendment, the Supreme Court decides the “standing” requirement based solely upon resolution of the substantive question of whether the claimant’s Fourth Amendment rights were violated.\textsuperscript{245} A claimant must show that “the disputed search and seizure has infringed an interest of the defendant which the Fourth Amendment was designed to protect.”\textsuperscript{246}

\begin{itemize}
\item \textsuperscript{239} Harwell, \textit{Doorbell-Camera Ring Firm}, \textit{supra} note 122 (“The high-resolution cameras can provide detailed images of not just a front doorstep but also neighboring homes across the street and down the block.”).
\item \textsuperscript{240} See Carpenter, 138 S. Ct. at 2220 (explaining “voluntary exposure” as a necessary requirement underlying the third-party doctrine).
\item \textsuperscript{241} See \textit{supra} pp. 23–24.
\item \textsuperscript{243} Id.
\item \textsuperscript{244} Id.
\item \textsuperscript{245} See \textit{Rakas v. Illinois}, 439 U.S. 128, 139 (1978) (“Rigorous application of the principle that the rights secured by this Amendment are personal, in place of a notion of ‘standing,’ will produce no additional situations in which evidence must be excluded. The inquiry under either approach is the same. But we think the better analysis forthrightly focuses on the extent of a particular defendant’s rights under the Fourth Amendment, rather than on any theoretically separate, but invariably intertwined concept of standing.”).
\item \textsuperscript{246} Id. at 140.
\end{itemize}
In *Rawlings v. Kentucky* (1980), the government convicted David Rawlings on charges of trafficking and possession of various controlled substances. At trial, he tried to exclude from evidence the drugs discovered during an unlawful search of his girlfriend’s purse. The Supreme Court held that Rawlings did not have standing to challenge the search or request relief because he did not have a reasonable expectation of privacy in his girlfriend’s purse. His girlfriend did, but he did not.

Application of this Fourth Amendment standing requirement has produced some peculiar results. For example, in *United States v. Payner* (1980), the IRS suspected that certain American taxpayers illegally concealed funds in the Bahamas. As part of its investigation, the IRS devised a plan to search the contents of a visiting Bahamian bank president’s briefcase. The IRS paid a woman $1,000 to go out to dinner with the bank president while his briefcase was left at her apartment. An IRS agent entered the apartment with a key provided by the woman and then searched the contents of the briefcase. The information collected eventually led to the indictment of Jack Payner for falsifying his tax returns.

At trial, Payner moved to suppress the evidence, claiming the IRS conducted an illegal search. The Supreme Court agreed that the search was illegal, but held that Payner did not have standing to complain: it was neither his apartment nor his briefcase that the IRS invaded.

---

247 448 U.S. 98 (1980).
248 *Id.* at 101.
249 *Id.* at 102 (explaining that the argument failed at the trial court level).
250 *Id.* at 104–05.
251 *Id.*
253 *Id.* at 729.
254 *Id.* at 730.
255 *Id.* at 741.
256 *Id.* at 730.
257 *Id.*
258 *Id.*
259 See *id.* at 735 (“Our Fourth Amendment decisions have established beyond any doubt that the interest in deterring illegal searches does not justify the exclusion of tainted evidence at the instance of a party who was not the victim of the challenged practices.”).
The requirement for Fourth Amendment standing makes it difficult to challenge dragnet surveillance programs like the NNW.\textsuperscript{260} The current doctrine takes a personal view of Fourth Amendment rights that focuses on individuals instead of “the people” as a whole.\textsuperscript{261} Broad, indiscriminate, and unreasonable surveillance programs cannot be challenged outright or on behalf of others without demonstrating a personal violation.\textsuperscript{262}

A plaintiff contesting the NNW on Fourth Amendment grounds would therefore need to assert that government access to Ring footage violated his legally recognizable (i.e., subjectively manifested and objectively reasonable)\textsuperscript{263} expectation of privacy. Admittedly, it will take time for the right case to come along and be recognized by a court—law enforcement accessed historical CSLI without a warrant for many years before the Supreme Court decided Carpenter.\textsuperscript{264}

Still, the scenario is not impossible to imagine. Consider the following hypothetical: Police receive an anonymous tip that Chuck is growing marijuana. The investigating officer sends a request for Ring footage in the area surrounding Chuck’s house. He receives a video of the exterior of the house from a Ring user in the community. The video reveals nothing pertinent, but the officer takes note that he received a helpful submission. Every two weeks, for the next six months, the investigating officer requests footage from the same area, because he continues to receive videos of the exterior of Chuck’s home. Finally, after six months of requests, the officer obtains a video that reveals Chuck smoking marijuana on his front porch. The officer uses this evidence to obtain a search warrant for Chuck’s home. Law enforcement searches his home and turns up nothing but a small

\textsuperscript{260} See David Gray, Collective Standing Under the Fourth Amendment, 55 Am. Crim. L. Rev. 77, 78 (2018) (explaining how Fourth Amendment standing rules “have set artificial constraints on who can challenge government searches; the ability of individuals and groups to challenge searches and seizures at the programmatic level; the kinds of evidence deemed relevant in Fourth Amendment cases; and the types of remedies litigants can pursue.”).

\textsuperscript{261} Id.

\textsuperscript{262} Id. at 78–79 (“Fourth Amendment standing . . . allows challenges only to individual instances of government action by those who have suffered a personal violation of their subjectively manifested and reasonable expectations of privacy.”).

\textsuperscript{263} Id. at 79.

\textsuperscript{264} Richard M. Thompson II, Cong. Rsch. Serv., R43586, The Fourth Amendment Third Party Doctrine 12 (2014) (“The difference in constitutional treatment between the content of a communication and its non-content addressing information dates at least as far back as the 19th century.”).
amount of marijuana. Law enforcement charges Chuck with possession of a controlled substance. At trial, Chuck moves to suppress the evidence.

The NNW allows for this kind of surveillance scheme. Following Jones and Carpenter, however, a court could arguably grant Chuck’s motion to suppress the evidence obtained by the Ring footage, seeing that the repeated, consistent, and covert police requests for video violated his reasonable expectations of privacy. When a scheme like this is available to law enforcement, it automatically imposes an “[a]wareness that the government may be watching.”265 Moreover, the ability to surveil citizens in this manner risks “run[ning] against everyone”266 as the NNW camera network proliferates.

B. Federal Cases

Examining the federal cases that involve surveillance technology and techniques analogous to the NNW helps illuminate how the court’s understand and apply the Fourth Amendment. Two lines of cases offer important insight: (1) Cases involving “pole cameras” (cameras placed on utility poles or streetlights) that constantly record video of a person’s residence;267 and (2) Cases involving “cell tower dumps” (the gathering of all cell phone numbers utilizing a specific cell tower).268

1. Pole Cameras

Most federal courts hold that long-term pole camera surveillance of the exterior of a home does not constitute a search, but other courts disagree.269 Typically, cases holding that pole camera surveillance of the exterior of a

265 Jones, 565 U.S. at 416 (Sotomayor, J., concurring).
266 Carpenter, 138 S. Ct. at 2218.
267 See, e.g., Moore-Bush v. United States, 963 F.3d 29 (1st Cir. 2020).
268 See, e.g., United States v. Adkinson, 916 F.3d 605 (7th Cir. 2019).
home is not a search argue that defendants lack a reasonable expectation of privacy because the outside of their home is exposed to public view. On the other hand, cases finding the use of pole cameras to be a search generally focus on the long-term and unblinking nature of the surveillance. The consensus on pole-camera surveillance is still unfolding, with only a single Circuit Court opinion, United States v. Moore-Bush (2020), reviewing the issue since the Supreme Court’s ruling in Carpenter.

In Moore-Bush, the First Circuit overturned the district court’s decision to suppress evidence obtained from a pole camera that continuously recorded the outside of the defendant’s house for eight months. The district court compared the evidence from the pole camera to the CSLI records in Carpenter, arguing that it gives an intimate view of a person’s daily life unlike information that could be obtained by simply being in public view. It argued that the aggregate features of constant video surveillance (i.e., the uninterrupted recording, the focus on the front of the house and driveway; the ability to zoom; and the creation of a digital log) breached a person’s reasonable expectation of privacy. Moreover, it argued that such surveillance can compromise core First Amendment rights because people are less likely to exercise “political, professional, religious, and sexual associations” when they know the government is watching.

On appeal, the First Circuit reversed, arguing that the district court’s comparison to Carpenter was inappropriate given that Carpenter’s narrow holding did not address other “conventional surveillance techniques.” The Court likened the pole camera to a security camera, which Carpenter explicitly included as an example of the surveillance technology not “call[ed] into question.” It also emphasized that what a person “knowingly exposes

---

270 See, e.g., Houston, 813 F.3d at 287–88 (holding that defendant failed to establish an expectation of privacy).
271 See e.g., Vargas, 2014 U.S. Dist. LEXIS 184672, at *27.
272 963 F.3d 29 (1st Cir. 2020).
273 Id. at 31.
275 Id. at 150.
276 Id. at 145 (citing Jones, 565 U.S. at 416 (Sotomayor, J., concurring)).
277 Moore-Bush, 963 F.3d at 31. (“Carpenter was explicit: (1) its opinion was a ‘narrow’ one, (2) it does not ‘call into question conventional surveillance techniques and tools,’ and (3) such conventional technologies include ‘security cameras.’) (quoting Carpenter, 138 S. Ct. at 2220).
278 Id.
to public view does not invoke reasonable expectations of privacy,” and that *Carpenter* did not abrogate this principle.\(^ {279} \)

The First Circuit granted a rehearing *en banc*, but the Circuit judges split 3–3 on whether the pole camera surveillance at issue constituted a warrantless search under *Carpenter*.\(^ {280} \) The Fourth Amendment question therefore remains unresolved. The opinion demonstrates that the scope of Fourth Amendment protections depends critically on how broadly a court interprets *Carpenter*, and whether it considers something as “new technology” or a “conventional surveillance technique.”

The Ring Video Doorbell is effectively a privately-owned pole camera that attaches to a home’s doorbell. For several reasons, it should be considered a “new technology” for Fourth Amendment purposes. First, treating “security camera” as a broad category of surveillance technology undeserving of Fourth Amendment protection disregards the innovation that makes certain video surveillance “differ in both a quantitative and qualitative sense from other[s].”\(^ {281} \) An obvious and fundamental difference exists between a camera that records gritty images to video cassettes, and a network of cameras equipped with High-Definition recording, night vision, smartphone integration, cloud storage services, and the potential for facial recognition.\(^ {282} \) The Court in *Carpenter* offers no indication of what it specifically contemplated in its understanding of “security cameras,”\(^ {283} \) but, nonetheless, it made clear that courts maintain a responsibility to consider when innovation creates “seismic shifts in digital technology” that calls for increased Fourth Amendment protection.\(^ {284} \) A network of pole cameras attached to doorbells may represent such a shift.

Second, homes that neighbor a Ring camera are subject to video recording indefinitely. In both *Jones* and *Carpenter*, the Court described “long-term monitoring” as a more severe burden to privacy, given that it provides

---

\(^ {279} \) *Id.* at 32.

\(^ {280} \) United States v. Moore-Bush, 36 F.4th 320, 360 (1st Cir. 2022) (Barron, C.J., concurring).

\(^ {281} \) *Riley v. California*, 473 U.S. 373, 393 (2014).


\(^ {283} \) *Carpenter*, 138 S. Ct. at 2220.

\(^ {284} \) *Id.* at 2219.
an “intimate window into a person’s life.”285 Knowing that the government may access Ring video footage of anything that happens in front of the home may risk “chill[ing] associational freedoms.”286

Third, the NNW provides an expanding network of video surveillance that risks “run[ning] against everyone.”287 Critical to the Court’s decision in Carpenter was that CSLI made possible the tracking of “not only [the defendant’s] location but also everyone else’s.”288 At the moment, sixteen percent of households in the United States—more than twenty million homes—own a video doorbell.289 Ring holds the majority of the market share,290 with more than 3 million cameras online.291 It averages two new partnerships with law enforcement agencies each day.292 Carpenter recommends closer Fourth Amendment scrutiny as these devices become ubiquitous.293

2. Cell Tower Dumps

Cell tower dumps provide “a download of information on all [wireless] devices that connected to a particular cell site during a particular interval.”294 By its nature, a tower dump involves access to much more user data than the historical CSLI at issue in Carpenter.295 The depth of the information revealed for any single person is not as significant, but it affects many more people. A

285 See Carpenter, 138 S. Ct. at 2217; see also Jones, 565 U.S. at 419 (Alito, J., concurring); id. at 415 (Sotomayor, J., concurring) and Carpenter, 138 S. Ct. at 2210 (“[CSLI] give[s] the Government near perfect surveillance and allow[s] it the ability to travel back in time and retrace a person’s whereabouts, subject only to the five-year retention policies of most carriers.”).

286 See Jones, 565 U.S. at 416 (Sotomayor, J., concurring).

287 Carpenter, 138 S. Ct. at 2218.

288 Id. at 2219.


290 Id.

291 Harwell, Home-Security Cameras, supra note 11.

292 Id.

293 See Carpenter, 138 S. Ct. at 2218 (“Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone.”).

294 Id. at 2220.

295 Emma Lux, Privacy in the Dumps: Analyzing Cell Tower Dumps Under the Fourth Amendment, 57 AM. CRIM. L. REV. 109, 109–10 (2020) (“[C]ell tower dumps collect cell-site location information from not one person, but from hundreds, or thousands of people.”) (footnotes omitted).
single tower dump can collect information from thousands of people. In the course of an investigation, law enforcement will typically ask for several tower dumps to determine if a device (or set of devices) was present at different locations of interest. In 2010, the FBI investigated a pair of bank robbers known as the “High Country Bandits.” Over the course of the investigation, the FBI received multiple tower dumps, totaling more than 150,000 individual cell phone numbers. Modern investigations routinely rely on tower dumps.

The Supreme Court explicitly declined to address whether tower dumps trigger Fourth Amendment protection in Carpenter, leaving it an open question as to how they should be regulated. In one of the only federal cases considering the issue since Carpenter, United States v. Adkinson (2019), the Seventh Circuit denied a motion to suppress evidence obtained from a warrantless cell tower dump. In its per curiam opinion, the court held that (1) by virtue of wireless carriers’ policy agreements, cell phone users consent to tower dumps; and (2) Carpenter does not cover tower dumps. Commentators, however, criticized this opinion as “highly dubious.” If user license agreements eclipse reasonable expectations of privacy, then they nullify Carpenter, because those agreements also include sharing historical

---

296 Id.
297 See Lax, supra note 295, at 109–10 (explaining how the FBI utilized tower dumps to catch the “High Country Bandits”).
298 Id.
300 Carpenter, 138 S. Ct. at 2220 (“Our decision today is a narrow one. We do not express a view on matters not before us [including . . . ”tower dumps.”]).
301 See Lax, supra note 295, at 113 (noting that Carpenter “explicitly left open . . . whether . . . acquisition of historical CSLI . . . like tower dump[s],” by the government triggers the Fourth Amendment).
302 See id. at 110 (recognizing that nearly all the cases that have considered tower dumps pre-date Carpenter).
303 916 F.3d 605 (7th Cir. 2019).
304 Id. at 610.
305 Id.
306 Id. at 611.
Moreover, although Carpenter declined to rule on tower dumps, the reasoning in Carpenter still applies to answering the Fourth Amendment question. The Seventh Circuit’s per curiam opinion weighs in on complex, important, and novel Fourth Amendment questions with a few paragraphs that “read[ ] like afterthoughts.” With little other legal authority on the matter, how cell tower dumps should be regulated is still an unsettled question.

The NNW provides an avenue for law enforcement agents to collect “video dumps” without a warrant. Law enforcement can ask Ring users in a specified area (up to 0.5 miles) for video footage within a specified time range (up to twelve hours). This dragnet structure offers the video analog of a cell tower dump, however, over-collecting video presents more serious privacy concerns than over-collecting CSLI. A single dot on a map hardly compares to video footage spanning up to twelve hours. Police forces across the country made more than 20,000 requests for footage captured by Ring cameras in 2020. Surely, some of those video dumps included intimately revealing or embarrassing content. As the NNW’s camera network expands and grows closer in scale to a cellular network, the privacy concerns related to over-collection likewise grow and the comparison to Carpenter is made stronger. Consider again the “High Country Bandits:” 150,000 cell phone numbers were collected to convict two individuals. In the context of video dumps, an error rate even approaching this magnitude is unacceptable. Carpenter measures privacy expectations based on the “nature of [the information] sought,” and whether it “runs against

308 See Cushing, supra note 308 (asserting that if user license agreements “waiv[e] . . . privacy protections . . . then the Carpenter decision no longer exists in the Seventh Circuit.”).
309 See Orin Kerr (@OrinKerr), TWITTER [Feb. 18, 2019, 3:57 AM], https://twitter.com/OrinKerr/status/1097419818498343618 (arguing Carpenter’s reasoning, though not directly on point, does help resolve the constitutionality of tower dumps).
311 See Lax, supra note 295, at 110 (recognizing that nearly all the cases that have considered tower dumps pre-date Carpenter).
314 See supra p. 23.
315 Harwell, Home-Security Cameras, supra note 11.
316 Lax, supra note 295, at 116.
317 Carpenter, 138 S. Ct. at 2219 (citing Miller, 425 U.S. at 442).
everyone.” Accordingly, the “deeply revealing nature” of video content, “belonging to persons [not] under investigation,” suggests that requesting a video dump through the Ring Law Enforcement Neighborhood Portal should require a warrant.

***

The above constitutional analysis suggests that modern Fourth Amendment jurisprudence can constrain the NNW. Carpenter limits the scope of the public view doctrine and the third-party doctrine, suggesting that Ring footage, like historical CSLI, should be protected by a search warrant. The doctrine of Fourth Amendment standing will make it difficult for a court to immediately recognize a person’s reasonable expectation of privacy in Ring video footage, but only because it will take time for the right plaintiff to come along (one suffering a personal violation of his reasonable expectation of privacy). A strong case for protecting Ring footage with a warrant can be made even in light of the standing requirement.

Moreover, the federal cases involving analogous technology illustrate applications of the current Fourth Amendment framework that would constrain the NNW. Ring hosts a network of privately-recorded video surveillance footage. To gain access to this network, law enforcement should be required to obtain a warrant, especially as the network grows and approaches the scale of a cellular network.

While courts continue developing the Fourth Amendment jurisprudence on video surveillance networks, some communities are heeding to Justice Alito’s calls to action in Jones and Carpenter, and enacting legislation that attempts to “gauge changing public attitudes, draw detailed lines, and to balance privacy and public safety in a comprehensive way.” The next section briefly examines some of the available legislation on video surveillance.

---

318 Id. at 2218.
319 Id. at 2223.
320 Id. at 2218.
321 See supra pp. 20–27.
322 See supra pp. 27–30.
323 See supra pp. 27–30.
324 See supra pp. 30–36.
325 Jones, 565 U.S. at 429–30 (Alito, J., concurring).
IV. VIDEO SURVEILLANCE LEGISLATION

Currently, no federal legislation addresses surveillance cameras.326 This vacancy pushes lawmaking responsibility to states and municipalities. As of January 2021, at least twenty-five localities have passed regulations limiting law enforcement’s video surveillance or requiring increased oversight.327 Of this group, fifteen enacted Community Control of Police Surveillance (CCOPS) ordinances.328 CCOPS is a model bill drafted by the ACLU, which requires more transparency and democratic approval with respect to the use of surveillance technology.329 Eight guiding principles underlie CCOPS:

1. Surveillance technologies should not be funded, acquired, or used without express city council approval.
2. Local Communities should play a significant and meaningful role in determining if and how surveillance technologies are funded, acquired, or used.
3. The process for considering the use of surveillance technologies should be transparent and well-informed.
4. The use of surveillance technologies should not be approved generally; approvals, if provided, should be for specific technologies, and limited uses.
5. Surveillance technologies should not be funded, acquired, or used without addressing their potential impact on civil rights or civil liberties.
6. Surveillance technologies should not be funded, acquired, or used without considering their financial impact.
7. To verify legal compliance, surveillance technology use and deployment data should be reported publicly on an annual basis.

327 STEVIE DEGROFF & ALBERT FOX CAHN, NEW CCOPS ON THE BEAT: AN EARLY ASSESSMENT OF COMMUNITY CONTROL OF POLICE SURVEILLANCE LAWS 2 (2021), https://static1.squarespace.com/static/5c1bfc7eece173955aceeb63b816d30a5eff89f2ce6894e1/1612984485653/New+CCOPS+On+The+Beat.pdf [https://perma.cc/9URX-EAY9].
328 Id. at 3.
(8) City council approval should be required for all surveillance technologies and uses; there should be no “grandfathering” for technologies currently in use.\textsuperscript{330}

While CCOPS’ ordinances are still in their incipiency, they are providing local communities greater insight into and control over law enforcement’s use of surveillance.\textsuperscript{331} For example, in San Francisco, activists sued the city’s police department for wide-ranging video surveillance of black-led protests. The police violated the city’s CCOPS ordinance requiring approval before using video surveillance for such a purpose.\textsuperscript{332} The ordinance provided activists with the only established mechanism for recourse.\textsuperscript{333}

CCOPS can and should be used by localities to provide insight into and control over the NNW.\textsuperscript{334} Police partnerships with Ring should be approved by city councils, and, if approved, the details of the partnership should be thoroughly explained to the public. Law enforcement should answer first to the communities it protects instead of a multinational technology company like Amazon.\textsuperscript{335} In this way, communities can regain power: they can decide the construct of “the new neighborhood watch” for themselves or ditch the idea altogether. Citizens that are disturbed by the partnerships between Ring and law enforcement should write their local legislator asking for increased transparency and constraints.

\textsuperscript{330} COMMUNITY CONTROL OVER POLICE SURVEILLANCE – GUIDING PRINCIPLES (ACLU)
\textsuperscript{331} DEGROFF & CAHN, supra note 328, at 2–3.
\textsuperscript{333} See id.
\textsuperscript{334} It should be noted, however, that CCOPS is not without its shortcomings, and it suffers from many administrative and enforcement problems. It takes time and energy to draft policies and reports, and the penalties for failing to follow policies are limited. Some scholars argue, for example, that it “shows gains in transparency but not necessarily a limitation on police power.” Andrew Guthrie Ferguson, Surveillance and the Tyrant Test, 10 GEO. L.J. 208, 259 (2021). Still, CCOPS ordinance can be useful and should be considered by interested communities.
V. CONCLUSION

In 1999, Universal Pictures released the American comedy, *Mystery Men*. The film is a mockery of comic book superhero collectives, like *The Avengers* or *The Justice League*. It features a unique character and aspiring superhero named “The Invisible Boy.” The Invisible Boy is determined to join the Mystery Men. In his audition, the leaders of the group ask candidly, “So let me get this straight, you have the ability to become invisible . . . but you can’t give us a demonstration?” The Invisible Boy responds earnestly, “I can only become invisible when no one is watching . . . [even if] I look at myself, I become visible again.” Confused and skeptical, the leaders ask, “How can you be certain you’ve achieved transparency at all?” The Invisible Boy answers decisively, “Well, when you go invisible, you can feel it.”

The New Neighborhood Watch imperils this superhero in everyone—the unique conscience and perspective—the superpower—that a person keeps only “when no one is watching.” Children are now warned: “[e]very time you ride your bike down [the] block, there are probably 50 cameras that watch you . . . If you make a bad choice, those cameras will catch you.”

This environment jeopardizes independent thinking and decision-making—the precise brand of citizenry that liberal democratic society assumes.

When an individual always conceives himself as being inspected, or cannot satisfy himself to the contrary, it causes him to internalize the norms

---

337 *Id.*
338 *Id.*
339 *Id.*
340 *Id.*
341 *Id.*

343 See Julie E. Cohen, *What Privacy Is For*, 126 Harv. L. Rev. 1904, 1906 (2013) (“Privacy is shorthand for breathing room to engage in the processes of boundary management that enable and constitute self-development. So understood, privacy is fundamentally dynamic. In a world characterized by pervasive social shaping of subjectivity, privacy fosters (partial) self-determination. It enables individuals both to maintain relational ties and to develop critical perspectives on the world around them.”); *Id.* at 1917–18 (“Citizens of [surveilled] society are not the same citizens that the liberal democratic political tradition assumes, nor do their modulated preferences even approximately resemble the independent decisions, formed through robust and open debate, that liberal democracy requires to sustain and perfect itself . . . The [surveilled and consequently] modulated citizenry lacks the wherewithal and perhaps even the desire to practice this sort of citizenship.”).
and expectations that he believes he will be judged against. Ultimately, the individual becomes his own overseer, ensuring the “automatic functioning of power.” This is what the Invisible Boy means when he loses his superpowers “[even if] he looks at himself.” In this fashion, the fundamental concept and model that underlies the NNW—that citizens should always be recording video of their neighbors to share with law enforcement—abrogates the first principle of liberal democratic society—that citizens engage in robust debate on the basis of individual ideas.

The Fourth Amendment plays a powerful role in preserving this American democratic tradition and it demands certain constraints to the NNW: at the least, that law enforcement requests for Ring video footage should require a warrant, just as requests for historical CSLI required a warrant in Carpenter. At bottom, the Constitution provides this much, but Courts move slowly, and communities seeking urgent safeguards should organize to enact local legislation.

The Framers understood the dangers of surveillance to freedom of thought and action and carefully restrained government overreaching with the Fourth Amendment. New surveillance technology and techniques should not erode this constitutional protection. Of course, as the Supreme Court has noted, “convicting the guilty will in every era seem of such critical and pressing concern that we may be lured by the temptations of

---

345 Id.
346 MYSTERY MEN (Universal Pictures 1999).
347 See Julie E. Cohen, What Privacy Is For, 126 HARV. L. REV. 1904, 1905 (2013) (“[F]reedom from surveillance, whether public or private, is foundational to the practice of informed and reflective citizenship. Privacy therefore is an indispensable structural feature of liberal democratic political systems.”).
348 See ELIZABETH HOLTZMAN & CYNTHIA L. COOPER, CHEATING JUSTICE: HOW BUSH AND CHENEY ATTACKED THE RULE OF LAW, AVOIDED PROSECUTION—AND WHAT WE CAN DO ABOUT IT 40 (2012) (“The framers of our Constitution understood the dangers of unbridled government surveillance. They knew that democracy could flourish only in spaces free from government snooping and interference, and they put restraints on government overreaching in the Fourth Amendment of the Bill of Rights . . . . These protections require, at a minimum, a neutral arbiter—a magistrate—standing between the government’s endless desire for information and the citizens’ desires for privacy.”).
expediency.” But it is “for that very reason [the Framers] insisted that law enforcement efforts be permanently and unambiguously restricted . . . .”

350 Id.