PRIVACY IN THE AGE OF SURVEILLANCE:
TECHNOLOGICAL SURVEILLANCE AND THE FOURTH AMENDMENT

ANTHONY P. PICADIO

FOURTH AMENDMENT OF THE UNITED STATES CONSTITUTION:

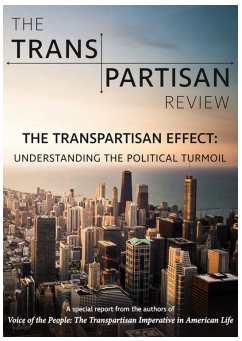
The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

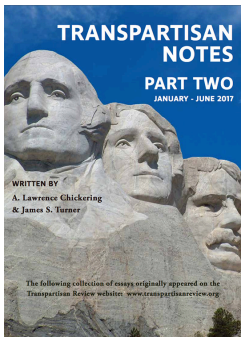
ABOUT THIS PROJECT

The Transpartisan Review's Stand-alone Series

A recurring feature of The Transpartisan Review (TTR) beginning in January 2019, TTR's second anniversary.

This series joins our weekly *Transpartisan Notes* series (now on note #115) begun July 4, 2016 and consists of important articles from the transpartisan community. The articles come from individuals such as *The Transpartisan Review's* advisors, colleagues, family, friends and commenters. We plan to publish such articles as they seem useful.





Thank you for your interest in *The Transpartisan Review*.

To receive notifications of our latest content,
send your email address to ***editor@transpartisanreview.com***.

THE TRANSPARTISAN REVIEW STAND-ALONE SERIES

IMPORTANT ARTICLES FROM THE TRANSPARTISAN COMMUNITY

OCTOBER 2019

Privacy in the Age of Surveillance

Anthony P. Picadio

James Otis, one of the most passionate and effective protectors of American rights.

The Transpartisan Review
Stand-alone Article #10

This article originally appeared in the October 2019 issue of the Pennsylvania Bar Association Quarterly.

MESSAGE FROM THE EDITORS

Individual privacy continues to be a major casualty of rapidly developing information technology. Google and Facebook, Amazon and Walmart, Verizon and Comcast all know more about us than we know about ourselves. New in-the-home devices sold by Amazon, Apple and others are said to listen in to our most intimate conversations. All of this data about individuals has become a commodity to be used, bought and sold by private enterprise and fuels a wide range of businesses.

Increasingly, law enforcement is using new technologies along with large databases containing information on individual citizens in developing policing systems which further reduce individual privacy. Much experimentation in the development of these new policing technologies is taking place at the local level, with cities such as New Orleans, Los Angeles, New York and many others trying to find the right technological surveillance solutions that works for their cities. The constitutionality of most of these new and evolving policing systems is yet to be decided by the Supreme Court.

We are pleased to publish today the following article by Anthony P. Picadio which traces the way The Supreme Court has applied the Fourth Amendment to the use of technological surveillance by law enforcement starting with a 1928 wire tapping case and continuing through the decision announced in June of last year involving cell site locational information obtained from wireless service providers. Mr. Picadio raises the question whether the Court's expansion of Fourth Amendment protection into the area of technological surveillance risks the continued development of more effective policing systems and suggests that the area might best be be left to local and state legislatures and to Congress to find the right balance between privacy and public safety.

The Right To Bear Arms: A Disfavored Right

by Anthony P. Picadio[1]

Abstract

It is not an exaggeration to define the times we are living in as the Age of Surveillance.[2] *Rapid and relentless advances in information technology, artificial intelligence, big data mining, high performance computing and visual and audio detection systems have placed in the hands of governments and private enterprise access to information about virtually every aspect of our lives: where we go, what we buy, with whom we communicate, what ideas and subjects attract our attention and what individuals, groups and organizations we associate with. The loss of an individual's ability to control access to this personal information has caused a substantial erosion of personal privacy. Of course, much of this loss of control over our personal information has been knowing, and at least arguably, consensual. However, the uses to which this information is being put are neither widely known nor understood and cannot fairly be characterized as consensual.*

Although technological advancements have eroded personal privacy, they have also produced substantial societal benefits. This is especially true in the area of crime control and prevention. Law enforcement can not only track the movements of criminal suspects with incredible accuracy, they also now have the capability to predict where crimes are most likely to occur and the most likely perpetrators and victims of those crimes.[3] *Very little attention has been paid to these beneficial aspects of advances in surveillance technologies. This lack of appreciation of the actual and potential benefits of new privacy-eroding technologies — the other side of the coin so to speak — is most noteworthy in United States Supreme Court opinions evaluating surveillance technologies under the Fourth Amendment.*

This article examines the way the Supreme Court has approached technological surveillance under the Fourth Amendment, points out the inadequacy of the analytical tests currently employed by the Court, and suggests a different approach. It raises the question whether the Court's current approach may do more harm than good by endangering the use and development of effective crime control and prevention techniques.

I. THE SUPREME COURT'S TECHNOLOGICAL SURVEILLANCE CASES

The principal vehicle by which the tension in our society between personal privacy and governmental surveillance is resolved is the Fourth Amendment to the United States Constitution as interpreted by the United States Supreme Court. The Fourth Amendment provides:

> 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.

Read literally, the Amendment protects against searches of houses ("the place to be searched") and the physical seizure of individuals or objects ("persons or things to be seized"). Digital information and internet communications are about as far removed from these concepts as one could imagine. A digital file is not really a "place," and a digital document is not quite a "thing." The words of the Fourth Amendment have to be stretched considerably to reach the digital world. The Court has been struggling with applying the Fourth Amendment to evolving means of surveillance since at least 1928.

a. The Pre-*Katz* Trespass Cases

Before 1967, the Fourth Amendment was pretty much home-bound. It was generally considered to limit the government's power to intrude upon the privacy of one's home. What occurred away from the home was fair game for unrestricted, government surveillance.

Chief Justice Howard Taft

For example, in *Olmstead* v. *United States* (1928),[4] the Court held that police wiretaps placed on telephone lines some distance from the home being surveilled did not constitute a "search" within the meaning of the Fourth Amendment because there was no physical entry into the defendant's home.

In *Olmstead*, several "bootleggers" had been convicted of violating the Prohibition Act on the basis of evidence obtained through extensive governmental wiretapping of defendants' telephone conversations. In a 5-4 decision, the Court held that the wiretaps did not constitute an unlawful search and seizure under the Fourth Amendment. Writing for the majority, Chief Justice William Howard Taft stated:

> The Amendment itself shows that the search is to be of material things—the person, the house, his papers or effects. The description of the warrant necessary to make the proceeding lawful is that it must specify the place to be searched or the person or *things* to be seized.[5]

This literal reading of the Amendment precluded its extension to wiretapping:

> By the invention of the telephone fifty years ago…. one can talk with another at a far distant place. The language of the Amendment cannot be extended and expanded to include telephone wires The Fourth Amendment is to be construed in light of what was deemed an unreasonable search and seizure when it was adopted.[6]

Although the term was not yet in general usage, the Taft opinion set forth an "originalist" interpretation of the Fourth Amendment as applied to technological surveillance techniques developed long after the Amendment's adoption.

Justice Louis Brandeis wrote a dissenting opinion in *Olmstead* rejecting Taft's originalist analysis and presenting what remains today perhaps the most eloquent argument in favor of a living Bill of Rights, one which adapts the concerns of the framers to modern times:

> Time works changes, brings into existence new conditions and purposes. Therefore, a principal to be vital must be capable of wider application than the mischief which gave it birth. This is particularly true of constitutions. They are not ephemeral enactments, designed to meet passing occasions. They are, to use the words of Chief Justice Marshall," designed to approach immortality as nearly as human institutions can approach it."[7]

Brandeis went on to observe that "[t]he progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping."[8] Already, "[s]ubtler and more far-reaching means of invading privacy have made it possible for the Government"[9] to spy on its citizens. For the Fourth Amendment to have any effect in protecting Americans from these technological advances in surveillance, it is necessary to look beyond the literal worlds of the Amendment to the fundamental purpose which those words were intended by the Framers to serve. And the Framers' purpose, in Justice Brandeis' words, was:

> [t]o secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and his intellect. They knew that only a part of the pain, pleasure and satisfaction of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right be let alone—the most comprehensive of rights and the right most valued by civilized man. [Emphasis added].[10]

Thus, over 90 years ago, Louis Brandeis found the right most longed for today, the right to be left alone, to be embodied in the spirit of the Fourth Amendment. However, five of the justices were not convinced and, by one vote, the holding of *Olmstead* became the law of the land; under the Fourth Amendment wiretapping without a warrant was constitutional.

Seventeen years after *Olmstead*, in *Goldman* v. *United States* (1942),[11] the Court held that the

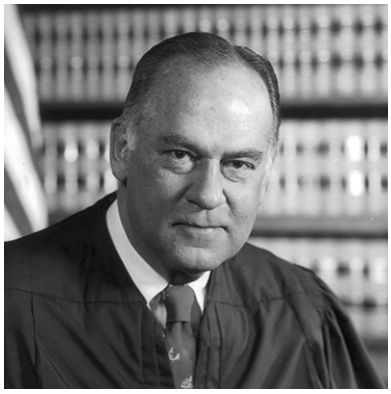
placing of a "detectaphone" on the outer wall of the defendant's office for the purpose of overhearing conversations within the room did not constitute a search under the Fourth Amendment because there was no physical intrusion into the defendant's premises.

The *Goldman* majority found *Olmstead* to be controlling and specifically declined the invitation to overrule it. Four justices, including Justice Frankfurter, were in favor of overruling *Olmstead*, but once again they lacked one vote. In an echo of the Brandeis *Olmstead* dissent, Justice Murphy, in dissent, wrote:

> The conditions of modern life have greatly expanded the range and character of those activities which require protection from intrusive action by Government officials if men and women are to enjoy the full benefit of that privacy which the Fourth Amendment was intended to provide.[12]

In *Silverman* v. *United States* (1961),[13] the Court reached a different result where police officers listened to conversations in an adjoining home by inserting a "spike mike" through a common wall. A unanimous Court held that an unconstitutional search occurred since the mike made contact with a heating duct on the other side of the wall, thus entering an integral part of the premises. As long as the surveillance technique did not cause a physical intrusion into the target's home (or other private space) the Fourth Amendment did not apply. But where it did, a search within the meaning of the Fourth Amendment occurred under the trespass doctrine of *Olmstead* and *Goldman*.

b. *Katz* v. *United States*



Justice Potter Stewart

This all changed in 1967 when the Court, in the case of *Katz* v. *United States*,[14] expanded the application of the Fourth Amendment beyond the home or other private space and applied it to prohibit the government from using an electronic listening device to eavesdrop on the telephone conversation of a bookie, Charles Katz, who was using a public telephone booth to place calls to gamblers in another state. In the process, the Court finally overruled *Olmstead*.[15] In *Katz*, the listening device was attached to the exterior of the telephone booth and did not intrude into the closed space of the booth. Nevertheless, the Court found that an unconstitutional search occurred. *Katz* was the first Supreme Court case to hold that a physical intrusion into a private space was no longer required to trigger the protection of the Fourth Amendment.

It is difficult to overstate the importance of *Katz*. Justice Potter Stewart, writing for a 7-1 majority, broke with prior case law which emphasized "the place" being searched and, in what was a truly revolutionary statement, said:

> [T]he Fourth Amendment protects people not places. What a person…. seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[16]

Although he took pains to say that the Court was not creating a generalized right of privacy ("The Fourth Amendment cannot be translated into a generalized 'right to privacy.'"[17]), that is exactly what it did. For the first time in our nation's history, a citizen had a constitutionally protected right to be free of government snooping wherever he/she was and wherever he/she went, so long as he/she took steps to protect his/her privacy. Justice Stewart found that Charles Katz had taken such steps when he shut the phone booth door behind him and paid the toll that permitted him to place the call.

Justice John Harlan, II, wrote a concurring opinion in which he stated:

My understanding of the rule that has emerged from prior decisions is that there 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."[18]

The Harlan concurring opinion is the genesis of the reasonable expectation of privacy test for which *Katz* is so frequently cited.

The Court declined to extend the Fourth Amendment's reach to a motor vehicle in *United States* v. *Knotts* (1983)[19] where the police surreptitiously placed an electronic device in a chemical drum, which a codefendant then placed in his car, to monitor its movements on public roads. The target did not own the drum; hence the placement of the device into the drum did not constitute a trespass. The Court said that tracking the movements of the car using the electronic device concealed in the drum did not amount to a search under *Katz* because a person has no reasonable expectation of privacy in his movements on public streets. ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.")[20]

c. Enter Justice Scalia: *Kyllo* and *Jones*

Justice Scalia was not on the Court when *Katz* was decided. While he recognized *Katz* as binding precedent, he was scathing in his criticism of its reasonable expectation of privacy test. In a concurring opinion in *Minnesota* v. *Carter*,[21] he derided the *Katz* test as a "fuzzy standard"[22] and a "self-indulgent test"[23] that had "no plausible foundation in the text of the Fourth Amendment."[24] For him, the language of the Fourth Amendment protected only the right of people to be secure in their "persons, houses, papers and effects."[25] That's all that the Framers wrote, and that's all that the Amendment protects.

Justice Antonin Scalia

So how would Justice Scalia, originalism's strongest proponent, apply what the Framers wrote to a case involving newly-developed technological methods of surveillance that the Framers could not have ever dreamed of? The first such case was *Kyllo* v. *United States* (2001),[26] where Justice Scalia wrote the majority opinion.

Kyllo involved the use of a heat detection device that was used to scan a house in which the owner was suspected of growing marijuana, which typically requires the use of high intensity, heat-generating lamps. The scan of the house was conducted by a federal agent from his vehicle parked across the street from the house and took only a few minutes. The device in question was non-intrusive, emitted no rays or beams and showed only a crude visual image of the heat being radiated from the outside of the house. It did not reveal conversations or other intimate details of the home. The scan showed that a side wall and the roof over the garage were relatively warmer than the rest of the home. Based in part on this evidence a federal magistrate issued a search warrant for the home, which was executed by federal agents who found an indoor growing operation involving more than 100 plants.

Justice Scalia began by pointing out that the visual observation of a home had always been considered lawful under the pre-*Katz* trespass test:

> The permissibility of ordinary visual surveillance of a home used to be clear, because well into the 20th Century, our Fourth Amendment jurisprudence was tied to common-law trespass.[27]

But what occurred here was no ordinary visual surveillance:

> The present case involves officers on a public street engaged in more than naked-eye surveillance of a home. We have previously reserved judgment as to how much technological enhancement of ordinary perceptions from such a vantage point, if any, is too much.[28]
>
> * * *
>
> The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy."[29]

He went on to hold that the technology utilized here went beyond the limits because the information it provided to the federal agent, concerning what was going on inside the house, could not have been obtained in the 18th Century without physically entering the house:

> We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' . . . constitutes a search—at least where (as here) the technology in question is not in general public use. This assures that degree of privacy against government that existed when the Fourth Amendment was adopted.[30]

In this interesting and clever way, Justice Scalia was able to connect the words of the Amendment

to modern technology by protecting that degree of privacy that those words created when they were first written. At the same time, he nudged the analysis back toward the trespass standard anchoring it to the language of the Amendment protecting privacy of "persons, houses, papers and effects." He paid homage to *Katz* in the process by referencing "the minimal expectation of privacy that exists, and is acknowledged to be *reasonable*" regarding the interior of the home.[31]

Kyllo was a 5-4 decision. Justice Stevens wrote the dissenting opinion which found the use of the heat detection technology entirely permissible under both the trespass test (detection of heat radiation did not involve"an unauthorized physical penetration of the premises"[32]) as well as the *Katz* test ("A subjective expectation that the [heat waves] would remain private is not only implausible but also surely not "one that society is prepared to recognize as reasonable"[33]). Heat waves, like cooking aromas, enter the public domain when they leave a building.

Kyllo is an endlessly fascinating case. It appeared that *Katz* had, once and for all, put a stake through the heart of the trespass test, but *Kyllo* gave it new life. In Justice Scalia's view, if it would have taken a trespass to acquire the information in the 18th Century, then the acquisition constituted a search under the Fourth Amendment.

Justice Scalia took another opportunity to move the trespass ball down the field in *United States* v. *Jones* (2012).[34] In this case, the government had surreptitiously attached a GPS device to the undercarriage of a car while it was parked in a public parking lot. Over the next 28 days, the government used the device to track the car's movements. The car's driver, Jones (the car was registered in his wife's name) was ultimately convicted of conspiracy to distribute cocaine. The conviction was based in part on the GPS-derived locations data which connected Jones to the co-conspirators' stash house.

As noted above, the Court had previously held in *Knotts* that the use of an electronic device to track a vehicle's movements did not constitute a search under the Fourth Amendment because a person had no reasonable expectation of privacy in his/her movements on a public street. But that case was decided before Justice Scalia was on the Court. In *Jones*, he continued his look-back to the 18th Century that began in *Kyllo*:

> It is important to be clear about what occurred in this case; the Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.[35]

He went on to say that a person's vehicle is among that person's "effects" which are expressly protected against government intrusion by the Fourth Amendment.[36] He squarely held that the property-based trespass test survived *Katz*, which he suggests would require a different result. He concluded that it was not necessary to decide the case under the *Katz* test because it could easily be

decided by application of the trespass standard. While he did not go so far as reversing *Katz* (a case which he previously said had no basis in the language of the Fourth Amendment), he did resurrect the property-based trespass test and obtained the votes of four other justices in doing so (Roberts, Thomas, Kennedy and Sotomayor).[37]

Justice Samuel Alito

Justice Alito wrote a concurring opinion in which three other justices joined (Ginsburg, Breyer and Kagan) which disagreed with Scalia's view that the trespass test survived *Katz*. According to Alito, *Katz* "finally did away with the [trespass] approach."[38] Having disposed of the trespass test, Alito was then confronted with the question of how tracking the vehicle's movements on public streets could be considered to violate *Katz* in light of the Court's previous holding in *Knotts* that a person in a car has no reasonable expectation of privacy regarding his/her location on the public streets. He did it by focusing on the duration of the surveillance, which took place during a period of four weeks. Justice Alito put it this way:

> [R]elatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable…. But the use of longer-term GPS monitoring in investigations of most offenses impinges on expectations of privacy…. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.[39]

Although he relied on the *Katz* test to decide that a search had occurred, Justice Alito recognized that the *Katz* test might prove difficult to correctly apply in this time of rapidly changing privacy expectations.

> [T]he *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology changes those expectations…. New technology may provide increased convenience opportunities or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the distinction in privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.[40]

Perhaps the most interesting aspect of *Jones* is the way Justice Sotomayor handled the issue of which test applied. She wrote a separate concurring opinion in which she agreed that both the trespass test and the *Katz* test were violated.[41] But she joined in the Scalia opinion rather than the Alito opinion. She therefore provided the crucial vote that revived the trespass test. Had she joined in the Alito

opinion the holding of the Court would then have been that the *Katz* case provided the only viable analysis under the Fourth Amendment.

Before turning to *Carpenter* v. *United States* (2018),[42] the most recent and most important Fourth Amendment case involving technological surveillance, it is necessary to run down two side streets so we can have a complete picture of the landscape.

II. THE THIRD-PARTY DOCTRINE

Twelve years after *Katz* was decided, the Court once again applied the reasonable expectation of privacy test, but this time the government won. In *Smith* v. *Maryland* (1979), the Court held that the government could install a pen register on the telephone company's property to record the telephone number dialed by the defendant.[43] The Court said that since Smith had voluntarily disclosed the dialed numbers to his telephone company so it could connect his call, he did not have a reasonable expectation of privacy in the numbers he dialed. This case follows *United States v. Miller* (1976), which held that a person has no reasonable expectation of privacy in information voluntarily given (or made available) to a third person.[44] As the Court stated in *Miller*:

> The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[45]

Justice Sonia Sotomayor

These two cases have established what has been labeled the "Third-Party Doctrine," which holds that a person has no reasonable expectation of privacy in information or things voluntarily given to a third party. The acquisition of such information by the government, therefore, is not a "search" under the Fourth Amendment. Under the Third-Party Doctrine, information which an individual voluntarily places in the control or possession of a third person automatically loses its protection under the Fourth Amendment without regard to that person's subjective privacy expectations. While the doctrine has its defenders, it has been criticized by a number of scholars and, more importantly, by a justice of the Supreme Court. In her concurring opinion in *Jones* (the GPS car tracking case), Justice Sotomayor had this to say:

> More fundamentally, it 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…. I would

> for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every web site they had visited in the last week, or month, or year…. I would not assume that all information voluntarily disclosed to some members of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[46]

III. THE BALANCING TEST – *RILEY* v. *CALIFORNIA*

In *Riley* v. *California* (2014),[47] the Court unanimously held that a warrantless search of the digital contents of an arrestee's cell phone was unconstitutional under the Fourth Amendment. Prior to *Riley*, the police were given wide latitude in conducting a search incident to a lawful arrest. Where the arrest itself was based on probable cause, a search of the arrestee's person required no additional justification. The leading case was *United States* v. *Robinson* (1973),[48] where an individual who was arrested for a traffic violation was subjected to a "pat down" by the arresting officer who found a crumpled cigarette pack in the arrestee's coat pocket. The officer opened up the crumpled cigarette pack and found several capsules containing heroin inside. The Court in *Robinson* held that it was not necessary for the arresting officer to obtain a search warrant before searching the cigarette pack because the search was incident to a lawful arrest.

In *Riley* (which involved two separate cases), arresting officers took possession of the arrestees' cell phones and searched their contents, including photographs, emails and other digital information. In deciding that it was necessary for the police to obtain a search warrant before conducting a search of the contents of an arrestee's cell phone, Chief Justice Roberts, writing for the Court, applied a balancing test:

> Absent more precise guidance from the founding era, we generally determine whether to exempt a given type of search from the warrant requirement "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[49]

Roberts emphasized that, unlike other objects that may be carried on an arrestee's person, a cell phone can contain a digital record of nearly every aspect of a person's life. As a result, a search of the digital contents of a person's cell phone is generally far more intrusive than a search for physical objects. Since the Court found that this serious intrusion into an individual's privacy outweighed the government interest in conducting a warrantless search, it held that a warrant was required before a police officer could conduct a search of an arrestee's cell phone.

Justice Alito wrote a separate opinion in which he concurred in the result but went on once again to express his misgivings about the desirability of courts deciding questions presented by rapidly developing surveillance technology:

> Many forms of modern technology are making it easier and easier for both government and

private entities to amass a wealth of information about the lives of ordinary Americans, and, at the same time, many ordinary Americans are choosing to make public much information that was seldom revealed to outsiders just a few decades ago.

In light of these developments, it would be very unfortunate if privacy protection in the 21st Century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment. Legislators, elected by the people, are in a better position that we are to assess and respond to the changes that have already occurred and that almost certainly will take place in the future.[50]

IV. THE *CARPENTER* CASE

Carpenter v. *United States* (2018) is the most recent, and, most important, case to date involving technological surveillance.[51] Unlike past cases, the facts of this case could not be stretched to fit the trespass test. This forced all of the justices to face the *Katz* test head on. As a result, there were five separate opinions (Roberts, Kennedy, Thomas, Alito and Gorsuch). First the facts:

Carpenter was convicted of being involved with others in a string of robberies of Radio Shack and T-Mobile stores, which took place in Ohio and Michigan. The prosecution introduced cell phone locational evidence obtained from Carpenter's wireless carriers, which showed, with respect to four of the robberies, that Carpenter was "right where the . . . robbery was at the exact time of the robbery."[52] The evidence, referred to as cell site locational information ("CSLI"), consisted of logs of time-stamped records showing each time Carpenter's cell phone accessed the wireless network, as well as the phone's location at that time. The records were owned by the wireless carriers, and they were produced to the government in accordance with court orders similar to subpoenas issued under the Stored Communications Act,[53] which were not issued based on probable cause. Chief Justice Roberts, writing for the majority, stated the issue presented to the Court as follows:

> This case presents the question whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements.[54]

At first blush, this case would appear to be governed by the Third-Party Doctrine. However, Chief Justice Roberts did not see it that way:

> [T]he fact that the individual continuously reveals his location to his wireless carrier implicates the Third-Party principle of *Smith* and *Miller* We decline to extend *Smith* and *Miller*…. to these novel circumstances. Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection.[55]

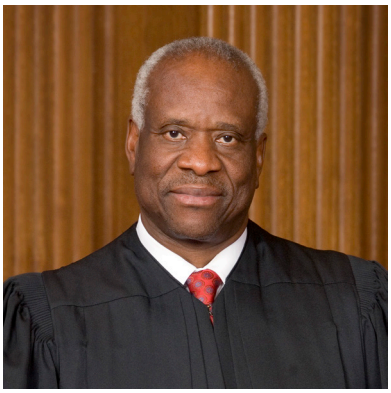
Roberts went on to announce a new rule that "an individual maintains a legitimate expectation of privacy in the record of his physical movements"[56] whether the government employs its own technology, as it did in *Jones*, or utilizes the technology of a third party, as it did in this case.

The chief justice has now staked out the strongest possible position favoring privacy protection in these technology-based Fourth Amendment cases. He wrote the opinion of the Court in *Riley*, he joined Scalia's majority opinion in *Jones*, and he authored the majority opinion in *Carpenter*. This is clearly an area on which he wants to place his mark. He even made a point of aligning himself with Justice Brandeis, the proponent of the "right to be let alone," by quoting from the Brandeis dissent in *Olmstead*:

> As Justice Brandeis explained in his famous dissent, the Court is obligated — as "[s] ubtler and more far reaching means of invading privacy have become available to the Government"— to ensure that the" progress of science" does not erode Fourth Amendment protection.[57]

There were four separate dissenting opinions in *Carpenter* (Alito, Kennedy, Thomas and Gorsuch), three of which make powerful arguments against the holding, reasoning and analysis of Roberts' majority opinion.

Justice Thomas argued for overruling *Katz* altogether and returning to an exclusive property-based analysis.[58] In his view, if you don't own it, you don't have any Fourth Amendment rights in it.[59] Since the wireless carriers owned their cell site records, Carpenter had no Fourth Amendment right protecting them from government intrusion.



Justice Clarence Thomas

Justice Thomas counted the ways that the reasonable expectation of privacy test has been criticized:

> Jurists and commentators tasked with deciphering our jurisprudence have described the *Katz* regime as "an unprecedented jumble," "a mess of contradictions and obscurities," "all over the map," "riddled with inconsistency and incoherence," "a series of inconsistent and bizarre results that [the Court] has left entirely undefended," "unstable," "chameleon-like," "notoriously unhelpful," "a conclusion rather than a starting point for analysis," "distressingly unmanageable," "a dismal failure," "flawed to the core," "unadorned fiat," and "inspired by the kind of logic that produced Rube Goldberg's bizarre contraptions."[60]

Justice Thomas' criticism of the *Katz* test is difficult to argue with. No one can seriously contend at this point that the *Katz* test serves any useful purpose other than providing a vehicle for some justices to "update" the Fourth Amendment to conform to their personal views of what limitations ought to

be placed on modern government surveillance. It certainly has no predictive value (every new case seems to be an exception to the rule enunciated in the last case); it clearly fails the law settlement function of the judiciary; it does not withstand thoughtful analysis (how does a court go about deciding what "society" considers reasonable?; is there really a unitary "society" holding a common view, or is society itself fractured, as is the Court, into factions holding opposing views?); and the *Katz* test does not take into account the potential harm to legitimate law enforcement that every incremental advancement of privacy can have.

It is this last point, potential harm to legitimate law enforcement efforts, with which the dissenting opinions of Justices Alito and Kennedy were most concerned. Justice Kennedy said this:

> The new rule the Court seems to formulate puts needed, reasonable, accepted, lawful, and congressionally authorized criminal investigations at serious risk in serious cases, often when law enforcement seeks to prevent the threat of violent crimes.[61]

Justice Alito, this:

> [I] fear that today's decision will do far more harm than good. The Court's reasoning fractures two fundamental pillars of Fourth Amendment law, and in doing so, it guarantees a blizzard of litigation while threatening many legitimate and valuable investigative practices upon which law enforcement has rightly come to rely.[62]

Justice Alito's major objection to the Roberts opinion was that it treats subpoenas for documents the same as searches and seizures under the Fourth Amendment. This, he thought, was inconsistent with precedent and would have far reaching adverse consequences for legitimate law enforcement efforts:

> Holding that subpoenas must meet the same standard as conventional searches will seriously damage, if not destroy their utility…. [T]oday the Government regularly uses subpoenas *duces tecum* and other forms of compulsory process to carry out its essential functions.[63]

Justice Alito went on to say that throwing a monkey wrench into the existing machinery of law enforcement by requiring probable cause for subpoenas of documents would stop many investigations at "the threshold of inquiry"[64] and, as a result, "a host of criminals will be able to evade law enforcement's reach."[65]

Both Justice Kennedy and Justice Alito would have applied the Third-Party Doctrine to hold that Carpenter retained no protectable interest in the cell site information he voluntarily placed into the hands of his wireless service providers.

The *Carpenter* holding is surprising. It rests on the premise that "society's expectation has been that law enforcement agents and others would not secretly monitor and catalogue [an individual's] every single movement."[66] That may be society's expectation in the case of an individual who is otherwise

not suspected of engaging in criminal activity. However, Carpenter was not such an individual. At the time law enforcement subpoenaed his cell site location records, Carpenter had already been identified by a co-conspirator by a participant in the string of robberies in question and had actually been placed under a valid arrest.[67] Moreover, unlike the situation in *Jones*, Carpenter's movements and location were not monitored in real time. Therefore, let us ask the question this way: Would society's expectation be that law enforcement should have access to historical cell site location records of an individual after he had been placed under reasonable suspicion of criminal activity and had actually been placed under a valid arrest for such conduct? The answer to this question is surely yes. At that point, society would not consider Carpenter's subjective intent to the contrary (if he actually had one) to be reasonable. What law enforcement did in *Carpenter* did not, in any way, jeopardize the privacy rights of the general public. The Court could very easily have said that an individual's cell site locational information may be accessed by subpoena under the Third-Party Doctrine where that person has been placed under reasonable suspicion of engaging in criminal activity and the basis for that suspicion can be demonstrated. True, reasonable suspicion is not probable cause. But the Court has, in the past, adopted a reasonable suspicion standard in a policing case.[68]

V. THE MOSAIC THEORY

In fairness to the chief justice and the other four justices who joined in his majority opinion in *Carpenter*, the majority did attempt to draw a line in order to prevent the catastrophe to law enforcement predicted by Justices Alito and Kennedy. The Roberts opinion drew it at the nature of the records in question. The holding covers only cell site location information ("CSLI") because of the particularly revealing nature of such information. The case was not merely about records documenting phone use. Rather, "it is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[69]

Chief Justice John Roberts

Carpenter is one of a trilogy of cases where the comprehensive nature of the information sought by law enforcement troubled the Court and led to the requirement of a search warrant.

The first case is *Riley* (2014), the cell phone search case discussed above, in which Chief Justice Roberts, writing for a unanimous Court, said:

> [A] cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record…. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions…. [T]he data on a phone may date back to the purchase of the phone, or even earlier….

> Finally, there is an element of pervasiveness that characterizes cell phones but not physical records.[70]

It was because of the ability of the data stored on a cell phone to paint a picture of a person's entire life that led the Court to require the police to obtain a warrant to search an arrestee's cell phone.

The second case emphasizing the ability of the data to reveal all aspects of a person's life is *Jones* (2012), also discussed above, where the Court held that using a GPS device to monitor a vehicle's location for a period of four weeks required a search warrant. Both Justice Alito and Justice Sotomayor emphasized the accumulation of details about a person's life which law enforcement obtained during the "long-term" tracking that was involved in that case.[71] *Carpenter*, of course, completes the trilogy.

This idea that if the data acquired by the government is sufficiently comprehensive or long-term to paint a detailed picture of an individual's life, then such acquisition constitutes a search within the meaning of the Fourth Amendment, has been referred to as the "Mosaic Theory" of data collection by the government.[72] Each individual tile in a mosaic tells us very little about what is depicted, but step back and view all of the individual tiles together and well, you get the picture. The Alito and Sotomayor concurring opinions in *Jones* essentially adopt the mosaic theory. The Roberts opinions in *Riley* and *Carpenter* also embrace it.

However, if the Court is truly concerned with the government's access to massive databases containing detailed and intimate information about individuals, it is difficult to see how it can draw and maintain the line at databases containing only locational information. Lay a subpoena on Google, for example, and you discover every internet search, every download, every email sent by subscribers of google.com (because Google actually retains a digital copy of each email) and much locational data. A subpoena on Google would produce information much more revealing than would a subpoena of wireless carrier's records.

Using many different sources of information, Google maintains location data on users of Android enabled smart phones that is far more detailed than what can be obtained from CSLI alone. CSLI information can place a person in the general vicinity of a building, perhaps within a city block. Google can place that person in a room in that building and follow him step-by-step as he moved through that room.[73] Facebook has enough information in its databases to profile well over one billion individuals in great detail. It would seem that the concern expressed in *Carpenter* about massive databases and their ability to reveal a detailed picture of an individual's daily life would apply with even greater force to companies like Google, Facebook, Microsoft and Amazon. Although extending *Carpenter* to these other companies might appear to be a good thing from a privacy protection point of view, it may, in the long run, not only make legitimate law enforcement more difficult, it may also retard the development and application of surveillance technologies which could prove effective in solving, preventing and reducing crime, and protecting potential victims of crime.

Under the Mosaic Theory as applied in *Carpenter*, when the extent of the surveillance produces sufficient information to present a complete mosaic, the Third Party Doctrine will not apply and the surveillance will constitute a search under the Fourth Amendment, triggering the search warrant requirement. In other words, the more useful to law enforcement the information becomes, the less likely it is that it can be used in an arrest or prosecution in the absence of a search warrant. This may prove to be particularly problematic in domestic terrorism investigations where early detection and capture are essential.

VI. THE REAL WORLD OF TECHNOLOGICAL SURVEILLANCE

Andrew Ferguson

Cell site location information like that used in the *Carpenter* case has helped law enforcement solve many crimes. A number of these are described by Andrew Guthrie Ferguson in his book on big data policing.[74] One of the more famous of these cases is known as the case of the "High Country Bandits." This duo of thieves robbed 16 small-town banks over the course of two years. One would enter the bank near closing time. He would brandish a gun in front of a teller, demanding and receiving all of the cash in the cash drawer. The second suspect stood watch. The FBI caught them by using CSLI from cell towers near four of the most rural banks. One Verizon cell phone number popped up near three of the four banks at the time the robberies were occurring. The FBI also determined that this phone communicated with another phone also near two of the banks at the times in question. The FBI then took those numbers and were able to locate the phones near the remaining bank robberies, again using CSLI obtained without a search warrant. The High Country Bandits were apprehended, removed from society and their crime spree was stopped.[75] According to Ferguson:

> In the United States, police have used cell-tower searches in thousands of criminal cases. In some instances, police simply subpoenaed the phone numbers from cell phone companies, and in other cases the police directly intercepted the cell phone number using "cell site simulators."[76]

In his book, Ferguson catalogues the many ways law enforcement is using large databases and algorithms to predict not only where crime is likely to occur, but also who is likely to be a perpetrator and who a victim. What is actually going on in the world of cyber surveillance makes the concern with cell site location information seem naïve and even downright silly. For example, Ferguson reports that AT&T has for years maintained a massive database of telephone metadata in searchable form. A record of every telephone call passing through AT&T switches is maintained in this database:

> Without a judicial warrant, law enforcement can obtain targeted information using an administrative subpoena or equivalent judicial order. This metadata connects the dots of social networks and locations of people suspected of criminal activities.[77]

Not only can law enforcement track an individual's whereabouts over the past five years using this data, it can also learn the identities of each person with whom the target interacted, along with the frequency and duration of each such interaction. How about that for creating a detailed mosaic of an individual's life!

Big data and artificial intelligence are being used by the police right now in a number of cities to identify bad apples and remove them from society through prosecution. The use of these high-tech policing systems has been effective in reducing crime rates. In New Orleans, Palantir Technologies, a private American company that specializes in big data analytics for governments, designed a system that integrated all existing policing and public safety data in the city's records, along with details of the city's infrastructure. The new system was used to determine likely perpetrators and victims of crimes:

> Using crime-mapping software, particular violent hot spots were identified. Using social network analysis, particular individuals were identified as being most likely to be victims of violent crimes…. New Orleans analysts could identify particular individuals at risk for violence…. Analysts using Palantir systems identified 2,916 individuals from the general New Orleans population of 378,750 most likely to be the victim of homicides.[78]

Using this data along with data identifying likely perpetrators, the city initiated 29 different outreach programs focusing on family, school, job training, etc., as well as more focused policing. The result was a dramatic decrease in homicides (29%) and gang murders (55%).[79]

New Orleans used data from its own records and publicly available information in constructing its system. Other police forces are integrating commercial databases into their policing systems.

> Enter…. the data brokers who have been collecting billions of bits of information about you, your family, and your home. Conveniently this information is arranged by address and accessible in real time for police responding to your home. The same folks who know you have stable credit, two kids, and a good job and like fine wine and cooking magazines, can also predict whether you will be a danger when you open the door.[80]

Similar data has been used by at least one police department to develop "threat scores" about addresses and the people who live there.

New York City has partnered with Microsoft to develop a system linking 9,000 closed-circuit surveillance cameras for real-time monitoring of lower Manhattan. The videos feed into a digital alert system that is trained to recognize threatening or suspicious behavior. Automated license-plate

systems record every car that enters the area and link to all of the information in the various included databases identifying the occupant/owner, his/her violation record, criminal record and threat level. The system also connects to terrorist databases.

> The recorded video can be replayed to track the direction, location, and movements of the suspect, and the technology can even search for descriptions, such as "all people wearing red shirts near the New York Stock Exchange." Still photos of matching people can be pulled up with one search, tagged to location, time and date.[81]

Automatic license plate readers ("ALPRs") have been in use for some time. They can scan a license plate and automatically compare it to a database of stolen cars, unpaid tickets or any other variable. As police cameras record license plates, a digital record is made containing the date, time and location of each license plate. Ferguson again:

> Over time the accumulated tracking of cars provides clues about travel patterns, habits, and the actual location of cars at certain times.[82]

Facial recognition technology is doing the same thing with faces. Cameras already in use in Los Angeles and other cities can scan a face 600 feet away and instantaneously compare it to photographs in its database that might consist of past mug shots, but that also might include a state's database of driver's license photographs. Ferguson:

> Like a car with a license plate, a person wanted for criminal activity can be automatically identified using facial recognition technologies. In addition, a digital map of past sightings is available for later investigatory use, so that should a crime occur near a camera, police can scroll back the video and identify all the people who walked past the camera at the relevant time.[83]

The FBI routinely uses state driver's license photograph data bases in its facial recognition surveillance system. According to a recent Washington Post article:

> [F]ederal investigators have turned facial recognition into a routine investigative tool. Since 2011 the FBI has logged more than 390,000 facial recognition searches of federal and local databases, including DMV databases.[84]

It has been estimated that the images of 50% of the U.S. population are in the database.[85]

As these policing systems develop, they add non-law enforcement data to their databases. Data from social services, foreclosures, social media, and even stored telephone records from pizza chains can all potentially be linked up. Photographs posted on Facebook, Instagram and What's App can easily enter one or more of the massive databases available to law enforcement.

We are not far off from the day when these systems will be able to solve many crimes almost

immediately. Linked camera systems with increasingly high resolution coupled with the right software can spot crimes in real time.

> Automated suspicion algorithms using artificial intelligence capabilities can turn surveillance cameras into digital spies able to recognize suspicious patterns and alert the police to the crime [s]mart cameras have been trained to look for patterns of suspicious activity, processing 60 billion instructions a second.[86]

That's what we already have. Here is what we very soon will also have:

> A single drone with sophisticated video, audio, and tracking capabilities could change crime patterns and privacy protections in one figurative sweep. While the technology does not quite exist yet, one would be hard-pressed to think of a crime that occurs in public that could not be observed and then investigated with an all-seeing drone.[87]

So, there you have it. Big data, Artificial Intelligence, drones, high-resolution video, and facial recognition, are all coming together to create automated policing systems having an effectiveness that could not have been imagined ten years ago. To be sure, these systems are not and will not be error free, and they have the potential to contain racial biases that cause them to focus disproportionately on minority communities.[88] These systems also have the potential for misuse. The same technology being used to solve and prevent crimes can also be used to find undocumented aliens and to watch protestors, dissidents and political opponents.[89] But, the potential for bias and misuse should not prevent us from taking maximum advantage of these advances in technology to create a safer and more secure country. Biases can, and no doubt will, be corrected,[90] and misuse can be legislated against. Moreover, any resulting loss of privacy from technological surveillance systems will not diminish all of the other constitutional rights we all have, such as freedom of speech, freedom of religion, the right against self-incrimination, the rights to liberty, due process and equal protection. We also have to consider the many errors and abuses that occur every day under our current policing systems. It is not as if the alternatives to technological policing systems have achieved human perfection. We should not throw the baby out with the bathwater and forego substantial benefits in crime solving and crime reduction in those cases where such benefits clearly outweigh the intrusion into personal privacy that such systems may cause.

This is especially true in domestic terrorism investigations. In the case of domestic terrorism, the ability of law enforcement to detect and capture mass shooters before they strike is essential. The use of technological surveillance techniques utilizing data in the hands of third parties may provide the best chance of early detection of mass shooters. If law enforcement is required to have probable cause and a search warrant in order to acquire such third-party data, many potential domestic terrorists will go undetected until they strike, and Justice Kennedy will be proven correct when he said that the holding of *Carpenter* will hamper "law enforcement when it seeks to prevent the threat of violent crimes."[91]

VII. NOW WHAT?

When one considers what is going on in the real world regarding the development and use of advanced technological surveillance techniques, and when one contemplates the potential benefits to society that can be realized from these technologies, the Supreme Court, as manifested in the various opinions written in *Jones* and *Carpenter*, seems to be concerned with almost trivial matters. The intrusiveness of the locational tracking presented in *Jones* and *Carpenter* pales into insignificance when compared to the policing systems already operating in New York City, New Orleans, Los Angeles and many other cities. Pervasive tracking systems utilizing drones, high-definition video, facial recognition and Artificial Intelligence are just over the horizon.

How will the Court deal with these new policing systems? Or, will it deal with them at all? Can the Court strike a proper balance between significant intrusions on privacy and the safety and security of the public? What analyses will it use to test these policing systems against the Fourth Amendment?

The Supreme Court

The one thing that can be said for certain is that the reasonable expectation of privacy test of *Katz* just doesn't work in this arena. How can someone have a reasonable expectation of privacy in any information obtained by any of these big data policing systems when it was either knowingly provided or publicly available? We all know these programs are ongoing, and many of us probably think they should continue. Justice Alito has recognized the changing nature of society's expectations of privacy as society itself becomes voluntarily enmeshed in the daily use of the very technologies that gather what used to be considered private information. But perhaps the greatest shortcoming of the *Katz* test is that it leaves out and doesn't consider the benefits to society from the policing or surveillance system under attack. At least this is true the way the Court has applied the *Katz* test. For example, in *Carpenter* and *Jones*, there is no evidence-based discussion regarding the impact on law enforcement of a warrant requirement. At the time *Jones* was decided, there existed over 3,000 ongoing investigations utilizing GPS tracking, all of which were terminated after the decision.[92] Under *Katz*, once the Court discerns a legitimate expectation of privacy that it feels society accepts as reasonable, the inquiry is over. Should it not be entitled to some weight that the surveillance system under consideration enabled the police to reduce the local homicide rate by 30 or 40%? If the Court stays in the business of evaluating these technological big data policing and surveillance systems, it should adopt an analysis that balances any diminution in privacy it perceives is being caused by the system against the societal benefits derived from it. The *Katz* test, as now applied, does not do that.

Perhaps, in place of *Katz*, someone will propose a balancing test like the one utilized in *Riley* (the cell phone search case) where Chief Justice Roberts, writing for a unanimous Court, utilized a test

that balanced "the degree to which [the search] intrudes upon an individual's privacy," against "the degree to which it is needed for the promotion of legitimate government interests."[93] It is difficult to understand why the balancing test could not have been used in *Jones* and *Carpenter* to weigh the benefits of long-term tracking against the privacy intrusion.[94] Three of the justices who joined in the majority opinion in *Carpenter* have never written in this area (Ginsburg, Kagan and Breyer). They each joined in Chief Justice Roberts' *Riley* opinion. Perhaps a five-justice majority can be cobbled together to replace the *Katz* test with a balancing test like the one used in *Riley*. Justice Alito, the former prosecutor, should happily join such a group because he has repeatedly recognized that the *Katz* test does not provide an optimal solution in these technological surveillance cases.[95]

Justice Thomas would reverse *Katz* outright and return Fourth Amendment jurisprudence to a pre-*Katz*, property-based analysis.[96] This would place primary protection of privacy in one's home and of one's person, papers and effects. It would eliminate the need for a third-party doctrine, but more than anything, it would take the Court completely out of the evaluation of these new technological surveillance and policing systems that the Founders could never have imagined. It would leave the field to Congress, state legislatures and local governments, i.e. society's elected representatives, to adjust the balance between privacy and beneficial policing systems. But more than anything, Justice Thomas' solution would ensure that the Court would not do more harm than good.

This article originally appeared in the October 2019 issue
of the Pennsylvania Bar Association Quarterly.

Endnotes

1. Anthony Picadio is a graduate of the University of Pittsburgh School of Law. His practice has been concentrated in the fields of Environmental Law and Commercial Litigation. He is a founder of the Pittsburgh firm Picadio Sneath Miller and Norton which, effective January 2018, was merged into the Pittsburgh firm Houston Harbaugh. Mr. Picadio is now of counsel to that firm.

2. *See*, Shoshana Zuboff, "The Rise of Surveillance Capitalism" (Public Affairs, New York, 2019). This book presents in startling detail the extent to which technological advances in computing power, Artificial Intelligence, data collection and mining and data analytics have created a new economic order with an insatiable need for more and more information about individuals and an ability to use this data to predict and actually modify human behavior.

3. *See* ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING (New York University Press, New York, 2017) This book describes the extent to which law enforcement is now using big data analytics and technological surveillance systems to identify and capture The book goes on to point out the dangers which can arise from biases and other sources of error inherent in some of these systems.

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

5. *Id*. at 464.

6. *Id*. at 465.

7. *Id*. at 472-3.

8. *Id*. at 474.

9. *Id*. at 473.

10. *Id*. at 478.

11. Goldman v. United States, 316 U.S. 129 (1942).

12. *Id*. at 138.

13. Silverman v. United States, 365 U.S. 505 (1969).

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

15. *Id*. at 353. The Court also overruled *Goldman*. *Id*.

16. *Id*. at 351.

17. *Id*. at 350.

18. *Id*. at 361.

19. United States v. Knotts, 460 U.S. 276 (1983). The electronic device used in *Knotts* was a beeper. The Court reached a different result in *United States* v. *Karo*, 468 U.S. 705 (1984) where a beeper was used to track a case of ether in a private residence removed from public view.

20. *Id*. at 281.

21. Minnesota v. Carter, 525 U.S. 83 (1998).

22. *Id*. at 92.

23. *Id*. at 97.

24. *Id*.

25. *Id*. at 92.

26. Kyllo v. United States, 533 U.S. 27 (2001).
27. *Id*. at 31.
28. *Id*. at 33.
29. *Id*. at 34.
30. *Id*.
31. *Id*.
32. *Id*. at 43.
33. *Id*. at 44.
34. United States v. Jones, 565 U.S. 400, 132 S.Ct. 945 (2012).
35. *132 S.Ct. at 949*.
36. *Id*.
37. Justice Scalia's opinions in *Kyllo* and *Jones* demonstrate that he was capable of adapting his theory of originalism to modern times and applying Fourth Amendment protections in circumstances the Founders could not possibly have anticipated.
38. *Id*. at 959.
39. *Id*. at 964.
40. *Id*. at 962.
41. *Id*. at 954-7.
42. Carpenter v. United States, 138 S.Ct. 2206 (2018).
43. Smith v. Maryland, 442 U.S. 735, 99 S.Ct. 2577 (1979).
44. *United States v. Miller*, 425 U.S. 435, 96 S.Ct. 1619 (1976).
45. 425 U.S. at 443, 96 S.Ct. at 1624.
46. Jones, *supra* n. 35. 132 S.Ct. at 957.
47. Riley v. California, 573 U.S. 783, 134 S.Ct. 2473 (2014).
48. United States v. Robinson, 414 U.S. 218 (1973).
49. Riley, *supra* n. 48, 134 S.Ct. at 2484.
50. *Id*. at 2497-8.
51. Carpenter v. United States, 138 S.Ct. 2206 (2018).
52. *Id*. at 2213.
53. 18 U.S.C. §2703(d).
54. Carpenter, *supra* n.52 at 2211.
55. *Id*. at 2216-7.
56. *Id*. at 2217.
57. *Id*. at 2223.
58. *Id*. at 2236, 2246.
59. *Id*. at 2235.

60. *Id*. at 2244.
61. *Id*. at 2223.
62. *Id*. at 2247.
63. *Id*. at 2246.
64. *Id*. at 2257.
65. *Id*. at 2256.
66. *Id*. at 2217.
67. *Id*. at 2212.
68. Terry v. Ohio, 392 U.S. 1 (1968) (stop and frisk).
69. *Id*. at 2220.
70. Riley, *supra* n. 48, 134 S.Ct. at 2489-90.
71. Jones, *supra* n. 35, 132 S.Ct. at 955, 964.
72. *See, e.g.* Owen S. Kerr, "The Mosaic Theory of the Fourth Amendment," 111 Mich. L. Rev. 311 (2012). The author, a leading Fourth Amendment scholar, criticizes the Mosaic Theory on the ground that there is no clear line delineating when the mosaic becomes sufficiently complete to constitute a search under the Fourth Amendment.
73. Zuboff, *supra*, n. 2 at 243-44.
74. *See* FERGUSON, *supra* note 3.
75. FERGUSON, *supra n.*3 at 107-108.
76. A cell site simulator, sometimes called a "stingray" device, mimics a cell tower and tricks cell phones into thinking it's an actual tower to which the cell phone reveals its unique identifier enabling the simulator to capture the cell phone's location. The federal government owns over 400 cell-site simulator devices, and the states own many more. These devices have been used to solve thousands of cases. FERGUSON, *supra* n.3 at 109-110.
77. FERGUSON, *supra* n. 3 at 114.
78. FERGUSON, *supra* n. 3 at 41.
79. *Id*. at 42. Ferguson describes predictive systems used or tested in various American cities that have reduced car thefts by 33% (Colorado Springs); shootings by 35% (Newark); burglaries by 25% (Los Angeles). While no scientific studies currently exist on the accuracy of predictive policing, two academic examinations of a predictive algorithm developed and sold by a company called PredPol, showed that predictive policing systems are at least twice as effective as systems using human crime analysis predictions. Id. at 64-70. But see, DailyMail.com, "AI experts from top universities SLAM 'predictive policing' tools . . ." July 26, 2019.
80. *Id*. at 84.
81. *Id*. at 86.
82. *Id*. at 88.
83. *Id*. at 89.
84. The Washington Post, "FBI, ICE find state driver's license photos are a gold mine for facial recognition searches," by Drew Horwell, July 7, 2019. [***link***]
85. Thedailybeast.com, "Half of US adults are now in facial recognition databases." April 13, 2017.
86. FERGUSON, *supra* n. 3 at 87.

87. *Id*. at page 105.

88. Facial recognition in particular has come under criticism as unreliable and more error prone the darker the facial complexion. San Francisco has prohibited its police force from using facial recognition pending further study. *See also*,"Facial Recognition's Racist History," The Privacy Project, NewYork Times, July 14, 2019, SR pg. 3. See Kate Conger, Richard Fausset, Serge F. Kovaleski, "San Francisco Bans Facial Recognition Technology," NY Times, May 14, 2019. [***link***]

89. The potential for misuse tends to be overstated. Surveillance alone will not abrogate or diminish the rights to protest, to assemble, to associate or to profess religious or political beliefs or to due process.

90. Facial recognition algorithms are constantly being improved. These improved algorithms have already caused "a dramatic increase in the accuracy of [facial recognition] technology." Nextgov.com, "How Facial Recognition is Changing CBP Operations . . .," July 26, 2019.

91. *See* note 61, supra.

92. Marc McAllister, "GPS and Cell Phone Tracking: A Constitutional and Empirical Analysis," 82 U of Cinn. L. Rev., Issue 2, 208, n.3 (2014).

93. Riley, *supra* n. 48 at 2484.

94. *See*, Amitai Etzioni, "A Cyber Age Privacy Doctrine," 80 Brook L. Rev. (2015), for a comprehensive balancing approach that considers the volume, sensitivity and the degree of cybernation of the collected data balanced against the common good, to determine whether a search has occurred under the Fourth Amendment.

95. It is not necessary to overrule *Katz* to make room for a balancing test. The second prong of the *Katz* test—an expectation of privacy that society accepts as reasonable—seems to cry out for a balancing test. But that is not how it has been applied.

96. So far, Justice Thomas has only Justice Gorsuch on his side. We have not heard from Justice Kavanaugh yet, so maybe, at most, three justices would vote to overturn *Katz*. There is, therefore, not much likelihood for an outright reversal of *Katz* any time soon.

This article originally appeared in the October 2019 issue
of the Pennsylvania Bar Association Quarterly.

ABOUT THE AUTHOR

Anthony P. Picadio

Mr. Picadio is a business litigator and environmental lawyer. He is listed as a Best Lawyer in Best Lawyers, Pittsburgh in the fields of Bet-the-Company Litigation, Commercial Litigation, Environmental Litigation and Personal Injury Litigation. Mr. Picadio is also listed in the 2008 through 2019 Edition(s) of Best Lawyers in America in Bet-the-Company Litigation, Antitrust, Commercial Litigation, Environmental Litigation, and Personal Injury Litigation (Defense and Plaintiff). His environmental law practice has involved contribution and cost recovery actions under CERCLA and related state statutes, air pollution regulatory enforcement and private damages actions, and water pollution issues.

Mr. Picadio is a former Pennsylvania Assistant Attorney General specializing in environmental enforcement matters and former chairman of an administrative tribunal charged with administering air pollution control regulations in the Pittsburgh region. He has served as an adjunct Professor of Law at Duquesne University School of Law and as a speaker at seminars on various litigation and environmental law topics. He has served on the boards of a number of non-profit corporations engaged in conservation and information technology projects.

THE TRANSPARTISAN REVIEW

THE TRANSPARTISAN REVIEW is a digital journal of politics, society, and culture, exploring the apparent disintegration of the traditional political, social and cultural order from a transpartisan point of view. This stand-alone article, and the series it belongs to, shares this exploration of the transpartisan impulse.

Direct inquiries to ***editor@transpartisanreview.com***.

Visit us online at ***www.transpartisanreview.org*** for more illuminating transpartisan discourse.