For Further Information Contact:
Public Information Office (202) 479-3211

JUSTICE JOHN PAUL STEVENS (Ret.)

The 53rd Henry J. Miller Lecture

Georgia State University College of Law
Atlanta, Georgia
April 16, 2014

In June of 1979, at the end of my fourth Term as a Justice of the Supreme Court, I provided one of the five votes supporting the majority's decision in *Smith* v. *Maryland*, 442 U. S. 735, the case holding that the Constitution does not require the police to obtain a search warrant to authorize the installation of a pen register to record the telephone numbers dialed from an individual suspect's home telephone. My vote in the case was influenced by my experience as a naval officer during World War II. Today I plan to say a few words about that work and then to discuss the question whether the considerations supporting the holding in *Smith* apply to today's practice of creating, using, and preserving a database including similar information about all of the telephone conversations in the United

States, including the millions that use cell phones that did not even exist in 1979.

I

In the summer of 1941, Leon Smith, the Dean of Students at the University of Chicago who was serving as a confidential recruiting agent for the United States Navy, provided me with the opportunity to earn a commission as an Ensign if I successfully completed the Navy's correspondence course in cryptography. One of the conditions of accepting that opportunity was an oath that I would never divulge either the existence of the course or the nature of my work for the Navy. Since Congress later enacted legislation that allows me to discuss that work today, I can tell you that I eventually received a letter inviting me to go the Great Lakes Naval Station to take a physical exam and formally apply for a commission. I did so on December

6th, 1941 and the Japanese responded by attacking Pearl Harbor the next morning.

While my correspondence course had provided me with training in how to read the text of encoded and encrypted messages, when I was on active duty I served as a traffic analyst, rather than as a decoder or cryptographer. The job of the traffic analyst was to obtain intelligence about enemy activities by monitoring his communications without reading their text — what today is often called "metadata" analysis. That skill is critically different from actually reading intercepted messages. Knowledge about the volume of the traffic in certain locations, identities of senders and addressees, their choice of codes, and the length and timing of their messages may enable the analyst to draw useful inferences; those inferences, however, are far less reliable or informative than intelligence gained by reading the texts of the messages themselves.

A dramatic event that occurred in April of 1943 when I was on duty as the traffic analysis watch officer in Pearl Harbor illustrates the vast difference between the two intelligence techniques. Intercepted traffic between the headquarters of the Japanese Navy's Commander-in-Chief in Tokyo and its Base Force No. 8 at Rabaul, New Guinea, persuaded us that the enemy was developing a response to its recent defeats on Guadalcanal. Our conjectures were replaced by specific information after our cryptographers succeeded in reading the text of one of those messages, which informed us not only that Admiral Isoroku Yamamoto - the architect of the attack on Pearl Harbor - would be making a morale-boosting tour of the area, but also provided us with the exact details of his planned flight from Rabaul to an airfield near Bougainville in the Solomon Islands. With the express approval of President Roosevelt, American aviators planned and executed an extremely difficult mission; they intercepted the Japanese flight and shot down

Yamamoto's plane. I was on duty at the time and remember reading a dispatch reporting on the downing of "one eagle" and a number of sparrows.

The difference between the quality of the intelligence obtained through cryptanalysis and the inferences obtained through traffic analysis is comparable to the difference between the intelligence obtained by listening to an intercepted telephone conversation and using a pen register to identify the parties to such a conversation. From the point of view of the participants to the conversation, there is a comparable difference in the magnitude of the invasion of privacy resulting from disclosures of the external characteristics of electronic messages and disclosures of their texts. The Japanese assumed - incorrectly as it developed - that we would not be able to read their encrypted messages, but they were certainly aware that we were monitoring their radio communications; they knew that we could, for example, use direction finders

to pinpoint the location of a submarine that broke radio silence while at sea.

Just as our enemies at war had a reasonable expectation that the texts of their communications would not be available to third parties, during peace potential criminals — like other citizens — reasonably assume that third parties will not listen to their telephone conversations. That expectation is protected by the requirement that the police must obtain a warrant before eavesdropping on such conversations. Those citizens are, however, well aware of the fact that telephone companies record the external characteristics of all of those conversations and that public agencies have access to those records to enforce rules relating to their supervision of the industry. When I first confronted the issue presented by the pen record case in 1979, I was immediately reminded of the vast difference between cryptanalysis and traffic analysis that was so important during the war against Japan. It seemed appropriate to me then - as it does

now - to recognize the same distinction during our ongoing war against crime.

The average citizen's expectations of privacy necessarily change in response to changes in society and changes in the law. The invention of the automobile, for example, enhanced freedom by giving individuals the opportunity to engage in a multitude of new enjoyable and profitable activities. But it also created new threats of personal injury by careless drivers and misuse by potential criminals. One of the public's responses to those threats was the requirement that every owner of a car obtain and display a license plate identifying him whenever the car is driven on a public street. That requirement facilitates the enforcement of traffic laws and the apprehension of persons engaged in criminal activity. It also impairs the value of the owner's interest in preserving the privacy of activities associated with the use of the car. Despite the license requirement's impact on privacy, it is now so familiar that few, if any,

persons question the conclusion that it is amply justified.

The fact that a new device - such as an automobile or a cell phone - may generate routine activities or new rules that give the public and the police access to information that a user of that device would prefer not to disclose is not a sufficient justification for imposing a warrant requirement as a pre-condition to police access to that information. Rather, in my judgment, it is part of the price that society pays for the benefits that the new device creates. The ability to refuse to take advantage of an invention is always a complete protection against the impairment of privacy that attends the decision to use it. By maintaining radio silence, the Japanese could have frustrated the work of our traffic analysts during World War II.

On the other hand, it is important to recognize that even though there is a vast difference between the quality of the intelligence available through cryptanalysis and that derived from traffic analysis,

the latter also is significant. I mention two details to support that conclusion. First, I was informed that the summary of the Japanese radio traffic during the preceding 24 hours that I prepared at the end of each of my watches was the first paper that Admiral Edward Layton, the Chief Intelligence Officer of the Pacific Fleet, read when he arrived in his office every morning. Second, the pen register that the police installed on the telephone line of the defendant in *Smith* v. *Maryland*, led to the apprehension and conviction of a criminal who might otherwise have gone free.

In sum, I remain persuaded that the value of the benefits obtained by the police as a result of their use of the pen register to investigate suspicious activities far outweighed the value of telephone users' interest in avoiding disclosure of the identity of the persons with whom they conversed on the phone. Mere suspicion, which is the basis for every police investigation, does not establish the probable cause

required to obtain a search warrant. A constitutional rule that required a showing of probable cause to justify access to facts identifying the parties to telephone conversations would impose a cost on the police that far outweighs its benefits to the general public.

II

Newspaper accounts of the present government's monitoring of telephone communications describe a program that differs from the use of the pen register in 1979 in both the magnitude of its potential invasion of interests in privacy and in its value for protecting public safety. Those differences have prompted debates about both the wisdom of the program and its constitutionality. Whether they support the conclusion that the program is unwise and should be modified or abandoned is, of course, different from the possible conclusion that the program is unconstitutional, and

that the *Smith* case should be overruled or distinguished.

The two most obvious differences point in different directions. The cost of the program is immense. Despite the efficiency and capacity of modern computers, the cost of maintaining and monitoring the database likely involves large expenditures, and almost certainly increases as the size of the program continues to grow. Like searching for a needle in a field of haystacks, that cost may well provide a sufficient justification for imposing significant limits on the scope of the program. On the other hand, the program is designed not to combat ordinary local criminal activity, but to prevent terrorist activity like the attack on the World Trade Center in 2001. The possibility of such an attack is real and the possibility that the program will lessen that danger is also real. Making judgments about the relative importance of those possibilities is obviously the business of our policy-makers rather than judges.

While neither the cost nor the potential value of the program determines its constitutionality, other differences between the program and the installation of a pen register may be relevant to the constitutional issue. First, unlike the police examination of the use of a single telephone for just a few days, the current programs involve the possible permanent retention of a massive quantity of records. The brief invasion of a single suspect's expectation of privacy is quite different from the on-going possibility that records in the database may one-day reveal private information about any of the millions of telephone users in the country. If measured by the number of people whose expectation of privacy is potentially at risk, or by the duration of that risk, the invasion seems unreasonable. But if it is measured by the likelihood that any particular individual - or, indeed, any group of innocent individuals - will be affected, the possibility is infinitesimal, and certainly not unreasonable.

Instead of choosing between those two possible approaches to the Fourth Amendment issue, it seems to me more helpful to focus on the threat to privacy that is posed by any additions to the database, or by government access to the database for the purpose investigating the use of a particular telephone. The reasoning that the majority endorsed in the *Smith* case in 1979 placed a zero value on the privacy interest because the identity of the persons called on the defendant's telephone - unlike what those persons said when they used the phone - was routinely disclosed to the telephone company (without any restrictions on its possible use) and therefore unprotected by the Fourth Amendment. That reasoning would also apply to each new addition to the database. The fact that many millions of additions to the database may be made on a daily basis does not, it seems to me, make the impact on any one individual any greater than the impact on the defendant in the *Smith* case.

But even if the Fourth Amendment may not require the issuance of a warrant before data is added to the database, perhaps it may impose some sort of barrier to official use of information that has already been accumulated. Such a judge-made rule might prohibit access to the data without probable cause to believe a subscriber is planning or engaging in unlawful activity. The effect of such a rule, in my judgment, would be profoundly unwise because it would render the database useless for the investigation of merely suspicious activity.

There is a distinction of constitutional magnitude between probable cause that is sufficient to support the issuance of a search warrant and mere suspicion that is sufficient to motivate police investigations but not sufficient to obtain a warrant. Using the database to identify persons calling or receiving calls from a telephone used by a suspected terrorist might help identify other potential terrorists without shedding any light on on-going or imminent criminal

activity. Even if those possible identifications might one day be valuable, that possibility would seldom, if ever, rise to the level of probable cause. Restrictions on access to information in the data base would impair its usefulness, and the introduction of a probable cause requirement might well frustrate critical investigations of suspicious activity.

My appraisal of the value of the public interest in avoiding the need to obtain a warrant to authorize either the continued addition of new information to the database or the use of information already included in the database returns me to the experience that affected my vote in the *Smith* case in 1979 and prompts this caveat. The inferences that a traffic analyst derives from the external characteristics of radio transmissions qualify as suspicious circumstances justifying further investigation, but seldom are themselves a sufficient basis for concrete decisions. Those inferences are far less reliable or useful than the facts that can be obtained from the use of other

intelligence techniques such as global positioning systems that can track the precise movements and location of vehicles. Because the data obtained from GPS sources is comparable to the text of intercepted messages both in its usefulness and its impact on privacy and is unlike the inferences obtained from pen registers or traffic analysis, what I have said about the latter does not apply to the former.

In sum, I remain persuaded that the *Smith* case was correctly decided in 1979 and that it supports the conclusion that the preservation and use of records identifying the parties to telephone conversations does not violate the Fourth Amendment. Whether the database provides benefits that are justified by its cost is an issue for others to debate. Historians may join forces with intelligence experts in opposition to reporters concerned with protecting the confidentiality of their sources during that debate, but it is a subject on which I am not prepared to comment today.

Thank you for your attention.