THOMAS E. FAIRCHILD LECTURE

PROTECTING THE FOURTH AMENDMENT SO WE DO NOT SACRIFICE FREEDOM FOR SECURITY

COLLINS T. FITZPATRICK*

The Thomas E. Fairchild Lecture
University of Wisconsin Law School
April 25, 2014 [1]

I want to thank the University of Wisconsin Law School and the Thomas Fairchild Lecture Committee for the honor and privilege of presenting this lecture. Tom Fairchild was a great friend from whom I learned much. He was a gentleman and a jurist and a giant at both, plus he was a lot of fun. I worked with him from 1971 until his death in 2007. If you do not know much about him, I recommend his Oral History, which is on the website of the United States Court of Appeals Library.[2]

After I was invited to speak, I gave a lot of thought to a topic that Judge Fairchild would want discussed. Let me tell you about my thought process and three experiences that brought me to my topic. As a young law student, I watched as Attorney General Elliot Richardson and Deputy Attorney General William Ruckelshaus resigned rather than follow President Nixon's order to fire Archibald Cox, the special prosecutor for the Watergate crimes. This was referred to as the Saturday Night Massacre. At that time, some of my fellow law students and I thought that President Nixon might be engaged in a *coup d'état*. We were wrong, and eventually Nixon resigned in disgrace, but he did resign. The Constitution worked.

---

* Collins T. Fitzpatrick is the Circuit Executive for the federal courts of the Seventh Circuit. He has held that position since his initial appointment when Thomas E. Fairchild was the Chief Judge of the Seventh Circuit. Mr. Fitzpatrick has his undergraduate degree from Marquette University and his law degree from Harvard Law School. He had a fellowship to work in legal services prior to his being a law clerk and then Senior Staff Attorney for the United States Court of Appeals for the Seventh Circuit.

1. The text of this piece is an edited copy of the 2014 Fairchild Lecture. I, the author, am responsible for all mistakes and omissions.

2. *The Oral History of Judge Thomas E. Fairchild*, LIB. U.S. COURTS OF THE SEVENTH CIRCUIT, http://www.lb7.uscourts.gov/OralHistories.html (last visited Nov. 8, 2014).

As a brand new lawyer, I represented a high school student at an expulsion hearing. The hearing officer was the assistant principal who also was the prosecutor of the charges. At the hearing, he added nine additional infractions to the two for which we had been given notice. The hearing officer/prosecutor introduced no direct testimony, only hearsay as to what others had told him. My client was expelled. The hearing denied my client the due process of law in many ways, but he was reinstated thanks to the decision of a federal judge. The Constitution worked.

Lastly, I was on Capitol Hill on September 11, 2001, and could see the smoke from the Pentagon. I listened to reports of another plane heading for Capitol Hill and the White House. Subsequently, our government did many things which in my view contravened our proud Anglo-American history of civil liberties. I certainly never thought that the United States of America would incarcerate persons for long periods of time without charges and a trial before an independent judge. Nor did I think that our government would institute torture policies to get confessions. The continuous question for all of us is: Is the Constitution still working?

Tom Fairchild was a great defender of civil liberties and the rule of law. As a candidate, he opposed Wisconsin Senator Joe McCarthy and as a lawyer he opposed McCarthyism. He advocated for civil rights before it was popular to do so. So I think that Tom would approve this message. In fact, he is probably sitting at heaven's equivalent of the Rathskellar having a beer and listening. All who knew Tom Fairchild enjoyed discussing with him serious issues like the Fourth Amendment as well as being entertained by his stories and jokes from the Tri County Bar Association Annual summer meetings.

One of the foundation stones for the rule of law and a democratic way of life is the Fourth Amendment. I want to address the issue of the balance between security and liberty: How do we protect people from harm while trying to make sure that the government's methods of providing that security do not deprive people of their liberty—their freedom from unwarranted privacy invasion by the government?

One of our great American leaders was Benjamin Franklin. He was a key delegate to the Constitutional Convention that wrote our Constitution. In 1775, while the 13 American colonies were still under British rule and a year prior to the Declaration of Independence, which Franklin also helped write, he said: "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."[3] Let me repeat that as this is a very important principle: "Those

3. *Two Messages from the Assembly to the Governor*, *in* AN HISTORICAL REVIEW OF THE CONSTITUTION AND GOVERNMENT OF PENNSYLVANIA: FROM ITS ORIGIN 289 (1759) [hereinafter *Two Messages*].

who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."[4]

There are two universal principles of the Fourth Amendment to the United States Constitution. The first principle is that "people [are] to be secure in their persons, houses, papers, and effects, [from] unreasonable searches and seizures."[5] The second principle is that "no warrants shall issue, [except] upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[6]

Two hundred forty years ago, there were no cell phones, Internet, cameras, planes, drones, knowledge of DNA, or Google Glass. There were no computers to keep track of all of the information. Nor was there a National Security Agency (NSA) or similar such foreign agencies to track all of this information.

The Fourth Amendment bans unreasonable searches and seizures and general warrants. It is not long, and it is not very detailed. How do the principles of the Fourth Amendment from the founding days of the American republic apply to our era of government searches of DNA data banks; recording of Internet and telephone traffic; facial recognition software with widespread camera coverage from flying drones and street level cameras; National Security Letter searches of health, utility, consumer, and financial records; and heat sensor searches of private spaces from public ways? How do we protect our citizens from those who would kill by coming to a gathering like this with an explosive vest or backpack?

Let's look at the history of the Fourth Amendment. Like many ideas that Americans think originated in the United States, the principles of the Fourth Amendment have a long developmental history. We in the United States have greatly benefitted from ideas developed throughout the world. Four thousand years ago, in Eschnunna, which is now modern day Iraq, there was a provision for death to burglars and exoneration of a person that slew the burglar coming into a person's home. In Byzantium, Roman Emperor Justinian's code provided that a freeman could not be summoned from his home, as it was "everyone's safest place, his refuge and his shelter." The principle developed is that there is one place where you are secure—your home.

The British were the most direct source of the principles enshrined in the Fourth Amendment. The British thought that a person's home was his castle and should not be violated without proper legal process. That idea initially appears in British legal literature in the 1300s. In *Semayne's*

4. *Id.*
5. U.S. CONST. amend. IV.
6. *Id.*

Case[7] in 1604, the British court recognized that a person could defend his home against entry by the king's agents unless there was proper notice.[8] A great British statesman, William Pitt the Elder, said:

> The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail—its roof may shake—the wind may blow through it—the storm may enter—the rain may enter—but the King of England cannot enter—all his force dares not cross the threshold of the ruined tenement![9]

The second part of the Fourth Amendment prohibits general warrants. Warrants to seize or search need to be specific. The government cannot search everyone's house for stolen money from a bank. There needs to be probable cause to think that the money is in a particular house or building. A famous British judge, Lord Coke, said that the background for the principle of no general warrants emanates from Article 39 of the Magna Carta and King John being forced by the nobles of his kingdom in 1215 to abide by the law.[10] Article 39 of the Magna Carta, which was issued as a result, provides: "No free man shall be taken or imprisoned or dispossessed, or outlawed, or banished, or in any way destroyed, nor will we go upon him, or send upon him, except by the judgment of his peers or by the law of the land."[11]

The British provided the doctrinal background for the Fourth Amendment, and the British were also the cause as to why the Fourth Amendment prohibited unreasonable searches and general warrants. The American colonists saw the British rulers as being unfair. The British government had for a long time used their laws to conduct general searches in homes, warehouses, and other buildings looking for untaxed goods, stolen property, seditious publications, criminals, military deserters, and vagabonds. In the American colonies, the British government looked for many ways to tax the colonists to support the colonial governments. Excise taxes on liquor, stamps, and other goods and custom taxes on imported goods were a mainstay of British government financing of the American colonies, and the colonists tried to avoid paying those taxes.

To combat tax evasion, the British and the American colonial governments used general warrants and writs of assistance to look for untaxed goods in homes and other buildings. General warrants were

---

7. *Semayne's Case*, (1604) 77 Eng. Rep. 194 (K.B.); 5 Co. Rep. 91 a.

8. *Id.* at 195.

9. *Miller v. United States*, 357 U.S. 301, 309 (1958).

10. WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 602–1791, at 109 (2009).

11. *Id.* at 109–10.

granted by a judicial officer to perform searches and seizures for a crime but did not specify particular locations. Writs of assistance were a general authorization to search for vagabonds, military deserters, and untaxed goods. Both legal documents authorized dragnet searches. Searches would be house-to-house and in the middle of the night for evidence of crime and suspects to arrest. These general warrants and writs of assistance were very much opposed by the Americans and they were the impetus for the Fourth Amendment prohibition against general warrants and the requirement that searches be reasonable.

How do you apply those principles to the surveillance and seizure techniques of today's world? The drafters of the Fourth Amendment wanted to require specific warrants and reasonable searches, and they applied them to more than a person's house. The Fourth Amendment provides that people have a right to be secure against unreasonable searches and seizures in their persons, houses, papers, and effects.[12] At the time, that list of persons, houses, papers, and effects was pretty all-inclusive of what citizens had. That was it: there were no extensive records or dossiers other than what a person kept, usually at their home. Houses included offices, shops, and barns.

The Fourth Amendment also contains a total prohibition against warrants unless issued upon probable cause by a judge, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized. Warrants had to be specific for the search and seizure and had to be based on probable cause—a legal term still in use today as the standard for arrest or search.

Over the years, the Supreme Court of the United States and other American courts have parsed the words of the Fourth Amendment. For example, eavesdropping devices were once allowed if they did not pierce the wall of the building. If they did pierce the building, such a piercing would have been a trespass to property. So if you could listen to a conversation inside a house from outside the house with a very sensitive listening device which did not pierce the wall, the Supreme Court of the United States, in *Olmstead v. United States*,[13] said that this was permissible, as it was not a trespass to the property.[14] Sixty years later the Supreme Court reversed itself in *Katz v. United States*,[15] holding that the defendant had an expectation of privacy which was violated by the warrantless electronic surveillance, even though there was no piercing of the wall.[16] The *Katz* Court did say that the evidence that the police had

12. U.S. CONST. amend. IV.
13. 277 U.S. 438 (1928).
14. *Id.* at 466.
15. 389 U.S. 347 (1967).
16. *Id.* at 359.

collected would have been sufficient to have obtained a warrant from a judge if the government had sought a warrant.[17] They just could not have used the eavesdropping device without a warrant.[18]

The Supreme Court's Fourth Amendment standards of a person's reasonable expectation of privacy and a person's right to be free from trespass have led to some interesting decisions. The Supreme Court, in *Smith v. Maryland*,[19] held that no warrant was required to install a pen register on the defendant's telephone, which indicated to law enforcement that the defendant had called the victim.[20] No warrant was required because the defendant had voluntarily disclosed to the telephone company whom he was calling.[21] Nor is a warrant required for bank records, as the customer voluntarily discloses this information to the bank.[22] Similarly, you disclose to businesses how much electricity you use and all of your credit card purchases. These records are obtainable without a warrant by the government under the theory that you already voluntarily disclosed the information to a third party, and therefore you no longer have an expectation of privacy in the information. But in *United States v. Jones*,[23] the Supreme Court held that a global positioning system (GPS) device attached to a car requires a court warrant.[24] It was the *Olmstead* trespass again, although some justices referred to the expectation of privacy.

In my opinion, the Fourth Amendment does not restrict the search of one individual who is under suspicion; it is the dragnet searching of millions of records by the government in order to find an individual that is objectionable. Courts have so parsed the Fourth Amendment that it is fine to obtain the records of all of us as we, like the plaintiffs Miller and Smith, disclosed the information to third-party companies. When courts so parse the words, they miss the point of the Fourth Amendment that there are to be no dragnet searches. Mass collection of data is a dragnet search. If the government wants to collect information on an individual suspected of a crime or gather information about possible criminal suspects, the prosecutor needs to explain to a neutral judge the basis for the warrant, i.e., the probable cause to issue the warrant. What is the evidence of a crime being committed by this particular suspect or the probable cause to believe that this type of search will lead to evidence of

17. *Id.* at 356–57.
18. *Id.*
19. 442 U.S. 735 (1979).
20. *Id.* at 742–43.
21. *Id.* at 743–44.
22. *United States v. Miller*, 425 U.S. 435, 440–43 (1976).
23. 132 S. Ct. 945 (2012).
24. *Id.* at 950–51.

the crime? The request for the warrant requires the prosecutor to focus on a particular person, place, effect, or thing to be searched or seized based on the crime being investigated, and the terms of the search need to be reasonable. Searches should be commensurate with the purpose of the search. Investigators should not collect DNA samples from all students in a school because one might have been involved in a rape, as the rapist wore a sweatshirt with the school's logo on it. A mosque should not be searched on Fridays when full of prayerful attendees, even though one of the congregants may be a criminal suspect. All phone records in a given area should not be collected to learn who is calling persons in Somalia or the Kurdish area of Iraq or the tribal areas of Pakistan. It is different if the records requested are for those of a person who is calling persons suspected of being threats to national security. Then you have probable cause to obtain a search warrant for the person's records.

In *Klayman v. Obama*,[25] District of Columbia Judge Richard Leon explains in detail how the NSA searches occur.[26] The government goes to the Foreign Intelligence Surveillance Court to get approval based on a suspected phone number or IP address. This first number is called the seed.[27] The records of numbers communicating with the seed are called the first hop.[28] Then the first hop numbers are searched to obtain their contacts.[29] This is called the second hop.[30] Then the second hop numbers are checked to obtain their contacts, the third hop.[31] You can get some idea of how many numbers are checked when I tell you that we are dealing with five years of records for each contact. If you estimate how many telephone or e-mail and Internet connections all of us have over five years, you have some idea of the massive amount of records which are searched by the time you get to the third hop. Judge Leon held that the program violated the Fourth Amendment as an unreasonable search.[32]

By contrast, eleven days later Judge William Pauley III of the Southern District of New York said that the program was constitutional in *American Civil Liberties Union v. Clapper*.[33] I commend these decisions to you, as well as the December 2013 Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies and the January 13, 2014, response to the report

25. 957 F. Supp. 2d 1 (D.D.C. 2013).
26. *Id.* at 14–19.
27. *Id.* at 16.
28. *Id.*
29. *Id.*
30. *Id.*
31. *Id.*
32. *Id.* at 42.
33. 959 F. Supp. 2d 724, 756–57 (S.D.N.Y. 2013).

incorporated in a letter to Senator Diane Feinstein from District Judge John Bates, former Chief Judge of the Foreign Intelligence Surveillance Court.

How do we apply the principles of the Fourth Amendment—reasonable searches and seizures and no general warrants—to the war on terror? In my opinion, the war on terrorism is not really a war unless the terrorists are being supported by an actual or pseudogovernment. In that case it is an actual war, and the existence of the nation could be at risk. In many instances we have citizens as well as foreigners who want to overthrow a government. Some revolutionaries are seen as good, and some are seen bad. Compare Thomas Jefferson, Kemal Ataturk, Mahatma Gandhi, Nelson Mandela, and Martin Luther King with Pol Pot of Cambodia and Charles Taylor of Liberia. Many people besides the then-current government officials saw the first group as terrorists, although now we all recognize the first group as heroes.

In times of real war, when a nation's security and existence is at stake, many rights are suspended. During the American Civil War, the writ of *habeas corpus* was suspended, military commanders did not seek court orders before searching buildings for enemy soldiers or supplies, and there was no right of trial by jury for captured persons suspected of being rebels. During World War II, loyal Americans of Japanese descent were forcibly removed from their homes and sent to internment camps. Their homes and farms were taken without due process of law. The formal apology from the United States and reparations many decades later did not make up for the denial of their liberty and property.

I mention this not because I am talking about wartime suspension of rights. I am talking about the application of the Fourth Amendment principles to today's "war on terror."

We all have access now to more total information than all the top government leaders had who were in office prior to 1970. You have at your fingertips on your smartphone or your iPad more information than can be found in print in the largest libraries of the world. I can check the weather in Istanbul for the next ten days or the seas in Papua New Guinea or elections in Ukraine. This is the result of the computer and the Internet. But like many inventions, they have good and bad points. We now have access to an infinite amount of information even if you are in the most remote location on earth or even in outer space. The disadvantage is that this technology also allows businesses to gather all sorts of information about you and share it with other businesses. And it allows governments to gather and store all kinds of information about you that it has already gathered, or to obtain it without notice to you. The government can collect this information without any court review using National Security Letters from businesses, such as your employer, cell phone company, Internet provider, credit card company, health provider,

bank, and many other businesses that gather information about you every day.

Even before I had a smartphone, which can identify where I am every day, I realized the power of this technology when I was skiing in Colorado with my family. I purchased my ski ticket with my credit card, which was then read by the chair lift attendant using a bar code reader. The chair lift only served expert ski slopes, so the information gathered could easily tell you how many times I went down the expert slopes and roughly what my speed was—definitely not as fast as any of my four sons. Although the government may have no use for that information, life and health insurance companies might be interested in my hobbies when determining my insurance premiums, or maybe my employer would not like my off-hours hobbies. Companies have not only a record of where you shop with your credit card but what you buy: liquor, cigarettes, ice cream, potato chips. I mention this because every day we give out a lot of information to others about how we live our lives. My elementary school teachers used to tell me that God is watching me. Well, God is getting a lot of help from the NSA and others watching all of us.

How does this relate to our topic? Well, is it permissible for the government to gather everyone's health records so that they can identify persons with social diseases? Or can the government access everyone's credit card records to match their expenditures to their declared income? What if the government collected records of everyone's purchases so that it knew everyone buying fertilizer, pressure cookers, remote control devices, and other potential bomb making equipment so it could cross-check them with records of regular participation in neo-Nazi and militia organizations?

How do we apply the Fourth Amendment to these types of government searches? We cannot turn back the clock. Information technology is here to stay, with its great potential to collect and store and cross-check information. It is one thing to have your cell phone company know whom you called and for how long, or your Internet company to know whom you are communicating with, or your credit card company to know how you spend money, but do we want to let the government have access to all of that information without suspecting us of a crime?

If you are looking for answers to the question of what searches a government fighting the war against terrorism should allow, I have no answers, but I can point you to the principles of the Fourth Amendment that have served us well: searches and seizures are to be reasonable, and the request for a specific warrant should be presented to a neutral judge based on probable cause that a crime has been committed, is being planned, or that this particular person committed a crime. There should be no dragnet searches, whether it be a search of everyone in this room or

a door-to-door search of houses, as was banned by the Fourth Amendment when it was drafted. Similarly, those Fourth Amendment principles also ban the government from collecting information on everyone because it might lead to evidence of a crime.

Edward Snowden is seen by many as a traitor to the United States for disclosing the secret methods that the NSA is using to collect information on Americans and others around the world. Others see Snowden as a great hero who did the right thing by disclosing what the United States is doing. History will judge. In any event, Mr. Snowden brought the issue to the forefront: Should there be any limits on a government's collection of information about its citizens in order to stop criminal activity? According to the reports, the NSA collects all of our Internet and phone conversations but only analyzes whom we contact, the length of the contact, and where the computers or cell phones are located. My understanding is that the text of the messages or the conversations are stored but not reviewed *unless* there is specific evidence that it is linked to a security threat.

I am sure that we will soon have, if we do not already have now, ubiquitous camera recordings coupled with facial identification software to identify where specific individuals were at a specified time.

Technology has provided the government the power to collect, store, and cross-check all kinds of records of citizens. I would venture to guess that there is a potential for the government to know much more about each of us than we can even remember. United States President Nixon and Federal Bureau of Investigation Director Hoover illegally collected information on opponents. I am reasonably certain that they would have used adverse information gathered under the current United States data collection programs as well. There are already persons arguing that the NSA records should be used to gather evidence on murderers, child pornographers, and drug dealers, or to find missing persons. How do you tell the public that the government gathers this information only on terrorists? I think it is reasonable to assume that if this information is gathered, it will be used legally or illegally for other purposes.

The wholesale gathering of telephone and Internet records is not limited to the federal government. The Wisconsin Supreme Court has under advisement the case of a defendant whose cell phone was tracked to his home by Stingray, a mobile device that state and local police use that mimics a cell phone tower and gathers the location of cell phones within range.[34]

The Fourth Amendment laid down two good principles: Searches and seizures are to be reasonable and there should be no general warrant dragnet searches. Remember what Benjamin Franklin said: "Those who

34. *State v. Tate*, 2014 WI 89, ¶ 7 & n.8, 357 Wis. 2d 172, 849 N.W. 2d 798.

would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."[35]

Thank you for this opportunity to speak to you today.

35. *Two Messages*, *supra* note 3, at 289.