Cite as Philip B. Heymann, 8 J. NAT'L SECURITY L. & POL'Y ___ (forthcoming 2016)

AN ESSAY ON DOMESTIC SURVEILLANCE

Philip B. Heymann[*]

INTRODUCTION

Whoever becomes president in the decades ahead may inherit extensive institutional knowledge (or the capacity to create such knowledge) about almost every citizen's beliefs, concerns, ambitions, interests, fears, actions, intentions, and associates. These multiple funds of information will also be readily subject to electronic search, storage, and combination and will generate increasingly reliable conclusions about our past as well as predictions about our future activities.

Should this scenario concern a far-sighted citizen? The possible ramifications for democracy and for civil society are dangerous. For instance, consider the importance of privacy of association. For an individual challenging a political or organizational leader, privacy of association is essential in the earliest stages of the challenge when that leader enjoys discretionary powers to help or harm the individual engaged in the challenge. Privacy of association was the issue in *NAACP v. Alabama*.[1] In this case, the State of Alabama demanded and sought to make public the membership lists of the local NAACP. Releasing these membership lists would have allowed private groups that were hostile to the political rights of black Americans to use that information as they chose[2]

[*] Philip Heymann is the James Barr Ames Professor of Law at the Harvard University Law School.
[1] 357 U.S. 449 (1958).
[2] At a hopefully rare extreme, many believe that the United States gave the names of leftists and Communist party members in Indonesia and Guatemala to military governments that were ready and willing to imprison or execute those named. *CIA and Assassinations: The Guatemala 1954 Documents*, GEO. WASH. U.: THE NAT'L SECURITY ARCHIVE, https://nsarchive.gwu.edu/NSAEBB/NSAEBB4.

On a more intimate basis, privacy is also necessary to shape one's behavior and self-image, free from social pressures. It limits how one's choices, including associations, affect others' attitudes about us—often a necessary safeguard in developing and projecting a chosen "self." The capacity of a government to use its surveillance systems to reveal what an individual is not yet willing to reveal denies our ability to choose our paths slowly and deliberately.

There is a second question, closely related to the first. Why, in an age of rapidly expanding use of the Internet and surveillance of that use by Internet service providers of various sorts, should we worry about the government? After all, the government probably gathers only a fraction of what private organizations do to learn about our interests, concerns, etc. for their commercial purposes, knowledge they use to create and sell new products and services.

The reasons are near at hand. Government surveillance has far greater reach. The FBI and other law enforcement agencies can – without any showing of a compelling social need (a predicate) or of a judicial warrant – do whatever private individuals are allowed to do to discover information. But they can do much more. They can demand, with the assistance of a federal prosecutor, any records that "might" be useful to a grand jury.[3] The government can be and is empowered to demand access to any records kept by third parties, including the vast array of electronic records now kept by businesses about their customers.[4] What private businesses can obtain by requiring a waiver of privacy rights as a condition of access to their services, the government can obtain without even that strained form of consent and without the alerting

[3] United States v. Williams, 504 U.S. 36, 48 (1992) ("[T]he grand jury can investigate merely on suspicion that the law is being violated, or even because it wants assurance that it is not. It need not identify the offender it suspects, or even the precise nature of the offense it is investigating.") (citations and internal quotation marks omitted); United States v. R. Enterprises, Inc., 498 U.S. 292, 301 (1991) (a motion to quash a subpoena on relevancy grounds "must be denied unless the district court determines that there is no reasonable possibility that the categories of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation").

[4] *See* Smith v. Maryland, 442 U.S. 735 (1979) (articulating the so-called third-party doctrine).

knowledge that consent gives to the individual being monitored. Indeed, notice can be forbidden with judicial approval.

The government is allowed to use informants and undercover agents in a way that is rarely available to businesses.[5] The government can and does develop technology, such as drones, which can greatly increase its powers to observe the activities of individuals from public spaces. The use of drones for surveillance is legal without any special showing of need and without getting a judge's certificate showing that a required predicate such as "probable cause" of a crime or a foreign danger has been met. With a predicate and a judicial warrant, the government can search places or activities, such as homes and electronic communications that no private individual can search without consent.

The government also has capacities to use information it acquires in ways far more frightening and more likely to be hostile than those of a company, like Google or Facebook, that seek to make you a loyal customer. It can turn suspicions into investigations, and investigations into an arrest and search with probable cause; it can deny discretionary benefits, insist on cumbersome formalities when you cross U.S. borders, and encourage the actions of others by making obvious its suspicion of, or attention to, particular individuals. It can acquire and store vast troves of data to be used for any of these purposes or for noncriminal forms of regulation.

I. THE FOURTH AMENDMENT GUARANTEE

For these reasons, among others, the Fourth Amendment to the United States Constitution restricts the surveillance activity only of governments when it guarantees that:

[5] *See* Hoffa v. United States, 385 U.S. 293 (1966) (the Fourth Amendment does not protect a voluntary statement of wrongdoing made to government informants based on a misplaced belief that that person will not reveal it).

> [t]he right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures shall not be violated.[6]

As constitutional law, the Fourth Amendment is intended to override any legislative or executive action which is inconsistent with its terms, that is, action which is "unreasonable" in light of legitimate expectations of privacy. Like the other provisions of the Bill of Rights it is therefore undemocratic in its unwillingness to allow changing forms of public opinion or shifting political majorities (like those that followed the ISIS attacks in late fall of 2015) to determine what privacy an individual enjoys.

The way the Fourth Amendment works is straightforward and generally understood by most Americans; its protections are surprisingly effective when supported by public opinion and judicial rules excluding from evidence any discovery made in violation of its terms.[7] To search any place, record, or communication protected by the Fourth Amendment requires, under existing Supreme Court doctrine and congressional statutes, a factual basis for thinking it probable (or, in some cases, for reasonably suspecting) that evidence of either a crime or a specified national danger will be found in a particular place (or in a particular communication). A court, having satisfied itself of such a "predicate," must certify that fact when it authorizes a search or electronic surveillance and it must specify the conditions under which surveillance may take place.

[6] U.S. CONST. amend. IV.

[7] Note that the analysis in this essay is limited to domestic surveillance. Separate rules apply to non-U.S. persons located abroad. Notably, Fourth Amendment protections apply to U.S. persons and to all persons on U.S. soil, but such protections do not apply to foreigners located abroad. United States v. Verdugo-Urquidez, 494 U.S. 259, 265-66 (1990).

The attributes and advantages of this system are immense. Consider six wonders of the Fourth Amendment:

(1) The system is entirely comprehensible, and the conditions under which it allows a search or seizure make perfect sense to a very high percentage of Americans who would never accept or trust the reasonableness of generalized demands for access to private information by government officials.

(2) The way it works makes unnecessary any substantial effort to establish in individual cases that the costs in terms of privacy of a particular search are less (or more) than the benefits to law enforcement or national security. It does not require an extraordinarily complicated balancing of the amount of damage a particular search does to privacy versus the amount of value it adds in terms of reduced crime or reduced danger to national security. While we might like to allow only those searches whose costs in terms of citizen insecurity are outweighed by their societal benefits in terms of solving or preventing a crime, the cost of making that judgment in the case of each individual search would be enormous.

Consider how difficult it would be to weigh each of the categories – costs and benefits – to determine where the balance falls. The cost to citizens' sense of privacy depends on, among other things, the current background or fears of governmental misuse of the power to search (e.g., before or after the Watergate scandals); and it also depends on whether the subject of the search was known or anonymous when the search took place, how sensitive the information to be acquired was, how private the location was where the information was found, how much was learned about a single individual, and how carefully the information was retained and not disseminated. On the other side of the balance, the benefits of surveillance are equally fact-dependent. They depend in each case on how dangerous the activity is that is subject to

surveillance, what alternative ways there are to learn about it, how useful (or alternatively unnecessary) the information likely to be found is in ending that danger, the inability of targets to find out about the manner of surveillance and thereby avoid it, and the likely promptness of discovery of evidence.

Any such costly analysis of the trade-off between costs and benefits of a particular search is replaced under the Fourth Amendment by simply requiring a showing that evidence of a crime or of a grave future threat would likely be found in the specified place or communication and at the time of the search or electronic surveillance. The police can quickly know what they are allowed and forbidden to do. Compared to detailed cost-benefit analysis in each individual case, the cost of this radically simplified balance is merely that a search is allowed even when the benefits of solving the crime may be relatively unimportant. Yet this does not detract greatly from the security individuals can feel under the Fourth Amendment.

(3) Use of Fourth Amendment standards provides important assurance of privacy to the vast majority of citizens, who are likely to know that there is not probable cause to search their places or monitor their communications.

(4) At the same time, it prevents foolish or abusive government searches, an important check on the efficiency and excesses of law enforcement.

(5) The system of the Fourth Amendment, unlike a grand jury subpoena for documents, does not tip off the suspect that he is about to be searched (and thus may decide to hide or destroy any evidence). The suspect takes no part in the decision of the court to issue a warrant.

(6) The Fourth Amendment manages to do these things without making known to the suspect, even after a search or an arrest, the identity of any informant who has decided to subject

a dangerous suspect to the risk of a search or electronic surveillance of his communications. The informant's identity may and will be kept secret.

Besides the Constitution, powerful political forces also support citizen privacy against unreasonable governmental intrusions, but that is not enough. The Fourth Amendment and statutes regulating electronic surveillance are needed for those situations and times in which fears or hatreds override the political support for privacy. The late 2015 period of fear of renewed terrorist attacks by ISIS was such a time.

II. THE LIMITS OF PROTECTION OF PRIVACY ACCOMPLISHED BY REQUIRING GOVERNMENTAL COMPLIANCE WITH THE FOURTH AMENDMENT

How then did the presidency come to command so much private information about each of us? Why didn't the Fourth Amendment prevent this? The answer can be explained largely in terms of a once-sensible definition of what is "private" as the opposite of "what is made public or knowingly exposed." As a matter of precedent, a category has developed of "no search" exceptions. These exceptions primarily consist of matters that are intrusions into what might otherwise be a "private" area but that are legitimized by the fact that the individual whose privacy has been invaded has already made the information "public," that is, "no longer private". The Fourth Amendment protects the secrecy of only those things or events that have not been made public and only against intrusions to which there has not been consent. That has seemed a natural interpretation of privacy. As we shall see, with the birth of new technology, that matter is far from clear.

But first let us return to the development of the idea that what has been made public and whatever information an individual has knowingly exposed to others are not private and

therefore are not within the protection against "unreasonable" searches furnished by the Fourth Amendment or, more generally, by privacy-protective statutes. The result of this understanding of privacy has been a list of types of surveillance which have been exempted from the Fourth Amendment requirements for whatever is a "search." Exemptions exist for surveillance from a number of locations that the suspect knows are available to the public and that can now be married to new technology to gather, store, process, and use vast new quantities of information that would have been private but for their willing exposure by the person now complaining of an unreasonable search.

Think of the following ways of obtaining evidence as a set of "platforms" for surveillance that are not subject to requirements of the Fourth Amendment. There are at least eight such "no search" platforms that governments and businesses in the United States have learned to exploit increasingly through new technology:

1. Informants
2. Undercover operations by government agents
3. Plain view from a place open to the public
4. Consent, very broadly construed, of the subject or possessor of the information
5. Records and information made available to a third party from whom the government obtains it
6. Subpoenas for records or testimony relevant to a grand jury investigation
7. Border searches
8. Searches incident to an arrest

The first five all rely on the fact that the surveillance is that of an individual who has, in some sense, willingly exposed the information publicly or consented to its exposure to particular individuals who turn out to be government agents. The last three platforms are based on considerations other than whether the information has been willingly made public. They are nonetheless platforms from which information that an individual believes is private can be searched without the basic requirement of a "reasonable" search and seizure: the showing of a basis for believing that a search in a particular place or of a particular communication will reveal either evidence of a crime or evidence of a foreign threat.

With the platforms I have just listed as embodying decades-old excuses from compliance with the predicate and warrant requirements of the Fourth Amendment, time and energy could once be saved by the "no search" interpretation, with apparently little cost in terms of reduced privacy and security. At least this was so prior to the burst of new surveillance technology. These "no search" categories are no longer justified by their harmlessness; now they are justified, if at all, only by the savings to the government in cost and time derived from bypassing the Fourth Amendment.

Consider the following four examples of a radically changed background for accepting or rejecting "no search" categories.

1. The "consent" rationale that justified the use of pen registers in the *Smith* case[8] — and the companion argument of "assumption of the risk" in talking to a government informant in the *Hoffa* case[9] – are simply inapplicable to the records kept electronically by Verizon, Google, Facebook, and many others. An argument that the individual has

[8] *Smith*, 442 U.S. at 742-743.

[9] *Hoffa*, 385 U.S. at 302.

consented to their being used by the record-keeper for such purposes as the record-keeper desires is simply fictional today. The "consent" form (as found in, for example, the "terms of service" of online companies) is produced by the business using it; it is rarely read; and there is little realistic alternative in the modern world for those reluctant to comply.

2. The exception to the Fourth Amendment for observations from a place open to the public made sense as long as the suspect could be assumed to have been aware of what he was exposing to the public.[10] It makes little sense when sophisticated thermal-detection equipment can tell what is going on inside a home the suspect thinks is sealed from view. Technologically remarkable lenses can see from a vast distance and to an extent that cannot be anticipated by an individual with any specificity. And what is whispered between individuals in a public space can be detected in ways that the suspect cannot anticipate.
3. The *Robinson* case held that the need to protect the officer making an arrest and to prevent destruction of evidence by the suspect were too difficult for an officer to appraise in the heat of making an arrest.[11] Therefore the slight privacy compromised by a limited search incident to an arrest did not justify the risks of requiring an officer to assess the dangers and the prospects of finding evidence, before searching incident to an arrest. But

[10] Under the plain view doctrine, individuals do not have a reasonable expectation of privacy if what was observed was visible to the public. The Court has applied the plain view doctrine to exempt from Fourth Amendment protections a variety of government observations made from places open to the public. *See, e.g.*, United States v. Karo, 468 U.S. 705, 713 (1984) (beeper placed on items when not in the home).

[11] United States v. Robinson, 414 U.S. 218 (1973).

the privacy cost of allowing a smart phone to be searched incident to any arrest makes the situation very different.[12]

4. A similar argument applies to border searches. Thus, arguments based on comparing the risk to law enforcement to national security of weakening either the historic claims of great inherent powers to protect a nation's border or of incurring costs of delay have already been weakened where the extent of invasion of privacy is far greater than at earlier times.[13]

In fact the burdens on police, prosecutors, and courts would not be greatly increased by carefully narrowing outdated rules for what is "not-a-search." The requirement of a warrant showing an adequate factual predicate for the government to demand or search massive records that have been obtained, under the implausible claim of consent, by a supplier of goods or services would not greatly increase the burden on courts, prosecutors, or police. The requirement of such a warrant wherever new surveillance technology allowed observation that has not been possible for ordinary citizens from a public place would not impose great cost or risks. The freedom to search a cell phone at the time of arrest or of a border crossing could, without great cost, be set aside and a return made to the Fourth Amendment's broader notions of probable cause and judicial certification of that finding. In short, the justifications for broad "not-a-search" doctrines

[12] *See* Riley v. California, 134 S. Ct. 2473 (2014) (limiting "incident to arrest" exception to warrant requirement for cell phone data).

[13] *See, e.g.*, United States v. Montoya de Hernandez, 473 U.S. 531, 540 (1985) (finding that an individual's expectation of privacy is less at the border than in the interior, and that "the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is also struck much more favorably to the Government at the border"). Note, however, that courts have so far declined to extend the *Riley* requirement of probable cause to searches of cell phones at the border. In *United States v. Martinez*, the district court held that a warrantless search at the border of a cell phone to collect phone numbers and text messages is permissible if supported by reasonable suspicion. No. 13CR3560-WQH, 2014 WL 3671271, at *4 (S.D. Cal. July 22, 2014); *see also* United States v. Blue, No. 1-14-CR-244-SCJ, 2015 WL 1519159, at *2 (N.D. Ga. Apr. 1, 2015). Even "invasive" or so-called "forensic" warrantless border searches of cell phones may occur on no more than reasonable suspicion. United States v. Saboonchi, 48 F. Supp. 3d 815, 819 (D. Md. 2014) (denying motion to reconsider).

have worn thin in an age of new technology at the same time as the use of them has opened broad new avenues for surveillance at a substantial cost to our privacy.

We will concentrate on the first five platforms and the long held view that what has been made public or knowingly exposed to a third party may no longer enjoy the protections of either the Fourth Amendment or of statutes against "unreasonable searches and seizures." In particular this essay will focus on the effects of new technology on the amount of information that can be gathered from the first set of five platforms.

III. THE HISTORY AND CONSEQUENCES FOR PRIVACY OF NEW SURVEILLANCE TECHNOLOGY

The new technologies of surveillance that exploit the platforms of plain view, consent, or information that has been accessed by a third party from whom the government obtains it have come about in two ways. *First*, they have been a response to the fear of renewed terrorism after the attacks on September 11, 2001. That fear brought the government into the business of developing new technology for monitoring from public places and also brought new authority to demand records from businesses with whom an individual has engaged in transactions of some sort.

Second, businesses have discovered the value of precisely targeted sales efforts. In particular, they have learned to gather information from an individual's use of the Internet in order to develop new products and services or to target their sales. This newly developed information has been available to the government because of provisions in statutes like section 215 of the Patriot Act, which very broadly authorized the government to demand the information. In many cases, businesses have simply volunteered the information.

The consequence of these developments has been to narrow sharply one of the two broad sources of privacy on which we have relied. Privacy against government surveillance has traditionally been protected in two distinct ways. First, privacy-protecting law, reflecting history and custom (such as forbidding a search based on a trespass unless it is justified by probable cause) is a creature of constitutional and statutory policy. A requirement of a predicate for surveillance limits when and where government surveillance can occur in a private place or of private communications.

But there has been another form of privacy that is at least equally important and applicable to places that have no legally established privacy protections, such as those based on notions of trespass. This second type of privacy allows individuals to take advantage of the laws of nature – to hide what they want to keep secret by using the privacy furnished by cover or distance.

New technology is rapidly narrowing this second form of privacy from government. The categorical exceptions to the applicability of the Fourth Amendment (that is, the law of "not-a-search") have become broad, open, and unpoliced avenues for search efforts. While officials have long been entitled to observe what is in plain view from a public location, dramatic changes are taking place in what can be seen from areas open to the public.

Like everyone else, government agents have been free to observe from public airspace thousands of feet above the ground,[14] but individuals on the ground could rely on the fact that little could be seen from that height. Now observations from great distances can detect much by using highly sophisticated lenses and other sensors. Moreover, modern surveillance retains a

[14] *See* California v. Ciraolo, 476 U.S. 207, 213-14 (1986) (plain view doctrine exempts public navigable airspace from Fourth Amendment protections); *see also* Dow Chemical Co. v. United States, 476 U.S. 227 (1986).

record of what was seen and thus can use what the inattention of a human viewer might have caused to be overlooked. And modern surveillance stores and archives what might otherwise have been forgotten.

Members of the public have long been legally entitled to spy from airspace 50,000 feet above the ground, but an individual's sense of privacy was unaffected because the individual knew that the vast majority of people couldn't get there and, even if they could, would be able to see very little from that height without very advanced and expensive technology. Privacy was protected by natural, technological, and economic limitations, not just by the law. But this is no longer true with a burst of new technologies that are available, as a practical matter, only to the government and a few others.

Nature provided, as a practical matter, an important opportunity for privacy – a very reasonable expectation of privacy – without the need of legal rules about what is a private place for a "search." In this area of "natural" privacy – either in places or in communications (or, as we will see, in records of one's transactions) – private individuals have long been allowed but unable to gather information. Government enjoys the same permission but not the same disability.

Adding surprising new government technology to the old legal authority (often based on the absence of a trespass) now allows the government to observe vast quantities of data that were formerly private. No new law has been necessary to grant immense new capacities for surveillance in the areas of such "natural protection." No new powers need have been granted in these areas. Privacy was reasonably expected if an individual had taken steps that assured that his neighbors and associates simply did not have the capacity or resources to observe what he had or was doing or saying. But that once reasonable expectation of privacy has now been

swallowed by the immense new governmental capacities to observe and store previously private information.

IV. THE SUPREME COURT RESPONDS

The developments described above have not escaped the attention of the Supreme Court. It has responded to the marriage of new technology to old legal categories of "not-a-search" by limiting the old "not-a-search" categories. Consider just a few examples:

1. Surveillance from a place open to the public is not a search.

    -- But there is a "search" if the government uses sense-enhancing technology, not in general use, to discover information regarding the interior of a home or its curtilage that could not otherwise have been obtained without a trespass.[15]

2. Use of a method of surveillance that is only capable of detecting contraband is not a search.[16]

    -- But applying it to what is in a house is a search.[17]

3. Taking advantage of consent granted for other purposes to engage in surveillance is not a search.[18]

    -- But it is a search if it applies to a house.[19]

[15] Kyllo v. United States, 533 U.S. 27, 40 (2001).

[16] United States v. Place, 462 U.S. 696 (1983) (a "canine sniff" by a well-trained narcotics detection dog at an airport does not count as a search within the meaning of the Fourth Amendment).

[17] Florida v. Jardines, 133 S. Ct. 1409, 1416-1417 (2013) (a "canine sniff" on the front porch of a home to investigate an unverified tip that marijuana was being grown in the home was a trespassory invasion of the curtilage of the home and thus counts as a search).

[18] *Hoffa*, 385 U.S. at 302; United States v. White, 401 U.S. 745 (1971).

[19] *Jardines*, 133 S. Ct. at 1416.

4. Using sophisticated technology such as a hidden beeper to gather information formerly obtainable without trespass by a conventional or technologically unsophisticated surveillance technique such as visual observation is not a search.[20]

-- But five justices have argued that it may be a search if the technology produces vastly more useable evidence.[21]

5. Generally any careless disregard of risks to your privacy will mean that the government's acquisition of information within that risk area is not a search.[22]

-- But it may be a search if what is disregarded is the possibility of high technology surveillance.[23]

In short, we have a set of relatively old concepts about what is not a search at all – a set that is no longer realistic. We have technologies that are allowing the exploitation of these doctrines in previously unimaginable ways – ways that are now being bought at the cost of the many advantages of the Fourth Amendment structure. Indeed, we have systematic exploitation of the "no search" categories.

We also have Supreme Court doctrine developing in a way that is intended to prevent the marriage of the "no search" categories to sophisticated surveillance technology, which the Supreme Court has sometimes defined as technology too expensive or too rare to be available to

[20] *Karo*, 468 U.S. at 712.

[21] United States v. Jones, 132 S. Ct. 945 (2012) (tracking movements for 28 days using GPS device attached to a vehicle without a valid warrant and without consent constituted a search); Riley v. California, 134 S. Ct. 2473 (2014) (search of a smartphone incident to arrest requires a warrant).

[22] California v. Greenwood, 486 U.S. 35 (1988).

[23] *Dow Chemical*, 476 U.S. at 238 ("It may well be . . . that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant.").

most of the public. And a reasonable remedy is at hand; the cost of the Fourth Amendment requirements of a predicate and a warrant is, at most, delay and much of the delay can be prevented with an emergency exception such as that which the electronic surveillance statutes include.[24]

V. ADJUDICATION AND LEGISLATION

A. Introduction

The path ahead seems clear for dealing with heightened powers of observation: follow the lead that the Supreme Court has begun to mark by narrowing the "not-a-search" categories and treating, as subject to the Fourth Amendment, any surveillance technology that defeats a "reasonable expectation of privacy" based on the limits of our senses as supplemented by very commonly available aides to observation.

Deciding that something is intrusive enough on reasonable expectations of privacy to be called a search, even if it falls into one of the "no search" categories, does not mean that our security will be threatened. Surveillance would still be allowed. It simply means that such surveillance must comply with the Fourth Amendment and, more generally, only invade privacy for good reasons often certified by a judge. The good reasons are the predicate required by statute or court decision.

The most important function of the Fourth Amendment is to moderate between our need for protection *by* the state against domestic and foreign dangers and our desire for the freedoms *from* the state that come with privacy. The Amendment manages to maintain an area of security

[24] *See, e.g.*, 18 U.S.C. § 2518(7) (providing that specifically-designated law enforcement officials may conduct electronic surveillance in emergency situations without a court order so long as they apply for a court order within 48 hours after the surveillance begins).

from state observation where, knowing of his own activities, an individual can also see that there is no likely justification for surveillance to be conducted on him (that is, there is no crime to be solved or foreign threat to be averted by such surveillance and thus no justified occasion for spying on the citizen himself.)

Specifically, a person can feel secure from a multitude of forms of social and governmental pressures to shape his thoughts, actions, and relationships in ways dictated to him so long as: his activities are not knowingly and casually exposed to the public (that is, the location is not open to public observation); he has not consented to the observation; and there is no reasonable basis for anyone to believe he is committing a crime or poses a foreign threat. The Fourth Amendment accomplishes this by requiring the government to have reason to believe that a search will lead to specified evidence of a particular crime or threat and often requiring that reason to be assessed by a neutral third party. A person can feel secure from search by knowing that he doesn't even *appear* to possess evidence of any particular crime or threat in a particular place and time.

The Supreme Court seems willing and able to move in this direction – at least where the issue is a greatly expanded capacity to observe. It has begun to narrow the fields of unregulated surveillance permitted by the "no search" doctrines wherever new technology allows these platforms to defeat very reasonable expectations of privacy.

A new restriction on either remote observation or surveillance through barriers traditionally promising privacy need not significantly increase the risk of a successful terrorist attack. There can be an emergency exception to any warrant requirement; and the predicate for remote observation can be less than probable cause. Observation of places where terrorist

activity is occurring will be prevented only when there is no reasonable, articulable basis for suspecting that activity in that place and at that time.

B. Legislation and Big Data

The Congress, rather than the courts, took the lead when the issue involved, not technologically enhanced powers to observe, but legally and technologically enhanced powers to access and search the files of third party businesses for records of transactions with suspected terrorists or their associates. Such search of third party files may be necessary to identify a terrorist relationship or a pending attack, for example, an order from ISIS to target a particular place or an offer by ISIS to provide the help of some of its supporters.

Under the provisions of the USA Freedom Act of 2015, the FBI can only apply for a court order for the production of third party records, papers, etc. concerning a U.S. person if the purpose is to advance an investigation to protect against international terrorism or spying.[25] Even then the court that is designated to order production can only issue that order if three conditions are established to its satisfaction:

1. That there are reasonable grounds to believe that the papers sought either:
    a. Are relevant to an authorized investigation to protect against international terrorism or spying; or
    b. Pertain to a suspected agent of a foreign power who is the subject of such an investigation.[26]

[25] *See* USA FREEDOM Act of 2015 §§ 101–07, Pub. L. No. 114–23, 129 Stat. 267 (2015).

[26] *Id.* § 101(a).

2. That what is to be produced is described by a "specific selection term," that is, a term that:
    a. Specifically identifies a person, account, address, or personal device and;
    b. Limits to the greatest extent reasonably practicable the scope of such things being sought, consistent with the purposes for seeking them (furthering an investigation to protect against international terrorism or spying).[27]
3. And, if the FBI is requesting the production of phone metadata on an ongoing basis (called "detail records"), that there is a reasonable, articulable suspicion that the required specific selection term is "associated with" an agent of a foreign power engaged in international terrorism or spying.[28]

C. Is the statutory protection too vague to create a sense of being secure in one's privacy? Is its privacy protection too broad for our security from attack?

Whether these provisions provide the full sense of security given by Fourth Amendment rights of privacy is less than entirely clear. The new statute ends the government's claims of statutory authority to demand bulk phone or other records on the ground that they may, at a later date, be found to include evidence for some future, as-yet-unspecified, intelligence investigation. The new requirement is for an authorized investigation and greater specificity is plainly demanded by the phrase "specific selection term."

[27] *Id.* § 201(b).

[28] *Id.* § 101(a).

What if the NSA demands all the metadata or credit card records for a particular past period on John Jones? The sense of security he once enjoyed from knowing he neither had, nor appeared, to have evidence of any crime or threat and thus could not be searched for that evidence is far less; the demand for third-party records, other than phone "detail records," requires only relevance– a very broad relationship– to an "authorized investigation" intended to protect against international terrorism or spying. The language of this power is very similar to that under which the NSA collected almost every record of almost every person using the phone. The difference is only in adding the word "authorized" to the former provision. It is hard to tell whether that will provide the security our hypothetical John Jones needs to trust that he is free of the risk of searches motivated only by politics or curiosity rather than by a reasonable belief that evidence of a crime will be found.

On the other hand, what if our intelligence agencies have reason to believe an anthrax attack is planned but know nothing more about its time, place, or likely perpetrators? A sensible step would be to check a list of customers of anthrax suppliers against a list of recent purchasers of equipment that could be used to disperse the anthrax. Identifying those in the overlap would be likely to present a manageable list of suspects for detailed investigation. The statute does not seem to allow this. Each of the two lists might fail the requirement of "specifically identifying a person, account, address or personal device."

CONCLUSION

A. The Shrinking of "No Search" Doctrines

The technological capacity for the U.S. government to know a great deal about almost every U.S. person – her activities, friends, interests, and much more – is growing very rapidly.

Either the growth of surveillance will pose a threat to an individual's sense of personal security and trust in the privacy of social and political relations; *or* government self-restraint will contain it, however secretly new capacities for surveillance are held; *or* legal requirements to show a need for certain information will limit it as has been true throughout much of our history since the adoption of the Fourth Amendment. The first is very dangerous to our freedoms; the second is unlikely so long as we face international and domestic dangers like those recently manifested by attacks in Paris and in California.

The third is, for the moment, unavailable because of a half-dozen or so now-obsolete doctrines defining what is *not* a "search" and is therefore *not* subject to the centuries-old legal requirements of having – and in many cases showing a judge – a demonstrated and serious need for surveillance of a place, a communication, or a record, *that is*, of honoring reasonable expectations of privacy. These doctrines provide unregulated and unrestricted platforms: for example, views from public places, records made and held by businesses or other associates, searches incident to an arrest, uninformed consent, etc., for the vast increases of what can be observed with the newest technology. The Supreme Court has been narrowing these platforms by requiring a predicate and a warrant for any surprisingly broad or intrusive observations technology has made possible.

That direction has been adopted in recent legislation regarding third party records as well. It will not greatly burden our investigators in demanding a showing of real need for any expectedly broad or intrusive technologically-enhanced surveillance. It would require only very traditional processes. That is a path well worth taking.

B. The Contest That Remains

The issues raised by the tradeoffs between privacy and security will remain with us. The demands of citizens for privacy and the needs of the government for surveillance of those posing potential dangers are inevitably in conflict along two dimensions.

First, there is and will continue to be a competition in technology. The technology of privacy will advance, largely funded by the private market for it, just as the technology of surveillance will advance, backed by governmental science and funding. Encryption is at least as powerful a technology of privacy as drones and high-powered lenses are of surveillance. There is no reason to think that the technology of secrecy is any harder to invent, distribute, and fund than the technology of surveillance. But there is one difference. If the technology of privacy is often inspired by the need to respond to new technological surveillance, there will always be a lag when surveillance has pushed ahead until privacy catches up. Indeed surveillance may not ever be discovered for some significant period.

Second, there will be a very complicated political and judicial competition in legal protection. For example, the Director of the FBI is demanding statutory protection of essential surveillance against the dangers of encryption. Meanwhile the leading providers of Internet communications maintain that they will be unable as well as unwilling to decrypt, at the government's demand, materials that the service providers have themselves encrypted for their customers; and are defending this power against legislative intrusions.

Here, prediction of the outcome may be more feasible than in the technological competition. The politics will depend on the extent of fear of enemies whose plans surveillance might discover. If the fear is reinforced by events (such as the recent ISIS attacks) and by political benefits from exploiting a threat (such as John F. Kennedy claimed from an alleged

missile "gap," George W. Bush from an alleged Iraqi plan to obtain nuclear weapons, or Donald Trump sought after Paris and San Bernardino), fear of foreign enemies will remain high. Fear of the government's prying is sporadic. Its discovery depends on classified methods of surveillance being revealed; and, even then as polls in late 2015 show, revelation of someone's secrets rarely creates the same degree of concern as the public feels about terrorist attacks.[29] New surveillance technology is more likely to be demanded by a public threatened by enemies than is new privacy technology likely to be demanded by a public fearful of its own government.

Finally, despite the trend of recent decisions, there is little reason to believe that the courts will vigilantly protect privacy in the face of surveillance that may be necessary to guarantee national security. Compliance with the rule of law is an exceedingly powerful political demand, and judicial decisions in the United States can trigger it. But fear for our national security is an even more powerful political force – one against which the courts have long been reluctant to test the power of law unless the clarity of legislative expression demands that the court act. Nothing in the language of the Fourth Amendment is that clear, and the statutes providing protection against electronic spying generally contain exploitable emergency exceptions.

[29] In November 2015, polls showed that seventy-two percent of Americans said "it is more important for the government to investigate terror attacks, even if that intrudes on personal privacy, rather than refraining from intruding on personal privacy." Greg Sargent, *Americans Fear More Terrorist Attacks, Want More War, and Don't Want More Refugees*, WASH. POST (Nov. 20, 2015), https://www.washingtonpost.com/blogs/plum-line/wp/2015/11/20/americans-fear-more-terrorist-attacks-want-more-war-and-dont-want-more-refugees.