LAWFARE RESEARCH PAPER SERIES

Vol. 3 May 10, 2015 No. 2

AN ESSAY ON DOMESTIC SURVEILLANCE

Philip B. Heymann[*]

[*] James Barr Ames Professor of Law, Harvard Law School. Professor Heymann served as Deputy Attorney General in the first Clinton Administration.

I. INTRODUCTION

A. FROM *ACLU V. CLAPPER* TO THE 4TH AMENDMENT

On May 7, 2015, a panel of the Court of Appeals for the Second Circuit held, in *ACLU v Clapper*, that Section 215 of the Patriot Act was not intended to authorize the United States government to gather telephone metadata on the sole basis that "they may become relevant to a possible authorized investigation in the future." In order use Section 215, the appellate panel said, the government would be required to show that records it seeks are relevant to an "ongoing 'systematic examination' of [a] particular suspect, incident, or group…"

This line of reasoning meant that the Second Circuit panel found it unnecessary to address the great difficulties and uncertainties of any general analysis of the constitutionality of the government's claim of statutory authority under Section 215. Yet it recognized that any new statutes addressing these issues will require addressing any concomitant 4th Amendment issues arising from them as well. What these 4th Amendment issues are, and how they might relate to the operations of any new or amended statutes, will both limit and clarify our options as a country and a society. These issues are the subjects of this essay.

B. THE SURVEILLANCE PROBLEM

Imagine a secure room in a secret government building. In the room sit five great computer engineers, five senior national security experts, and five fine lawyers. They have been assembled to protect our nation's security against terrorist attacks by using new technology for surveillance of terrorist suspects. The absences are as important as the attendees. No one has been invited to the meeting to raise and discuss issues about the effect on democracy or our trust in government of an enduring massive secret program of surveillance of most American citizens – in other words, something like the telephone metadata program authorized under Section 215 of the Patriot Act.

The engineers will worry about the effectiveness of what they propose. Assume they have proposals that will probably be "effective" in detecting some terrorist efforts. The national security experts will also worry about the cost; assume it is small compared to the overall budget for counterterrorism. That combination is likely to satisfy ten of the 15 attendees. What about the lawyers? They will worry about the legality and the reaction of the courts. Assume they conclude that an obscure statute, like Section 215 of the Patriot Act, or notions of judicial deference in national security areas, will make the program defensible or unchallengeable as a matter of law.

No one will feel responsible to ensure that the group discuss and consider the social consequences of the fears of American citizens likely to be aroused by such a massive and continuing program. Many citizens are already deeply suspicious of government and untrusting of secret judicial institutions and of a

congress that enjoys less than ten percent public approval. What's worse, the program may well endure whether or not is useful. It is unlikely to be cut off even if it produces no useful information, so long as that ineffectiveness is kept secret. Cutting it off would create grave political risks of revelation and of being accused of prying, wasting money, and, inconsistently, now endangering the American public. So there is likely to be little effort to monitor the effectiveness of the program and no effort to weigh the social effects. There will be no public criticisms unless the existence of the program leaks and, in any event, there is legal authority for it, which many will consider provides whatever moral or social legitimacy is needed.

Let us get deeper into the discussion. Where should it begin? The computer engineers have a variety of exciting ideas that may take a great deal of time to describe. The national security experts will have ideas about the likelihood of various attacks and what vulnerabilities to surveillance different terrorist tactics may involve. But even if the lawyers haven't focused on these issues before, they have – perhaps counter-intuitively to the general public – a starting place that will narrow the range of considerations and thus allow the conversation to proceed more rapidly.

If invited to speak first, the lawyers will say, "We must, of course, comply with the 4th Amendment to the U.S. Constitution, the 1st Amendment's rules on freedom of association and any applicable statutes regarding the privacy of communications; and we must accept judicial interpretation of these." But they will point out that there is a statute already on the books that "could" be construed as allowing a previously unheard-of massive surveillance of the phone metadata of almost all Americans. They are likely to note that, rather than rely on a contested interpretation of that authority by the executive, it would be much better for trust in our institutions if Congress were asked to approve whatever new proposals are developed. But there is often no way to seek clear legislative authority without revealing to our enemies what we are planning.

Having softened up their ten colleagues in this way, the lawyers are then ready to proceed to the good news. There are, the lawyers explain, a half dozen or more situations in which the Supreme Court has said that surveillance does not amount to a "search" – the category that the Constitution and statutes generally regulate. What's more, it is rare for Congress to have passed a statute regulating surveillance in these "not-a-search" areas, once the Supreme Court has said the surveillance does not raise Fourth Amendment issues. Congress did pass a law in this situation requiring some minimal conditions for using pen registers. But typically, when Congress does regulate surveillance that the Supreme Court has held is not a search, it has stopped short of requiring a showing of need for the surveillance in every case and for judicial approval – the core requirements of the U.S. Constitution.

The existence of "not-a-search" areas is critically important to making the burdens of authorization of surveillance manageable. "Not-a-search" areas free from regulation generally involve relatively innocuous forms of surveillance and

thus invite efforts to avoid cluttering the courts with unnecessary reviews of the justification in every case.

What hasn't been noticed, the lawyers explain to the group, is that these "not-a-search" areas have also turned out to be important to the legality of exploiting new surveillance technology. Using new technology in these areas now allows forms of surveillance that are far more secret, detailed, inclusive, and massive and far less regulated than our privacy laws would otherwise permit. And the digital fruits of this surveillance are subject to extremely productive forms of storage, analysis and processing that were never imagined at the time when these techniques of surveillance were ruled by the Courts to not be searches.

Finally, the lawyers produce a list of types of surveillance which traditionally law exempts from legal requirements for whatever is deemed a "search" – surveillance platforms that can be married to new technology to gather, store, process and use vast new quantities of previously private information. They explain that today the seven most promising such "legal" platforms for surveillance are:

1. Informants
2. Undercover operations
3. Plain view from a place open to the public
4. Consent (even unconsidered or constructive)
5. Subpoenas for records
6. Information made available to a third party from whom government obtains it
7. Border searches
8. Searches incident to an arrest

This story is of course fictional in its description of organization, location, and thought processes[1] -- but not in recognizing the effects of combining remarkable new surveillance with very old rules on what is "not-a-search" under the law protecting privacy.

The new problems of surveillance could have been addressed by bringing into the room where decisions are made a highly influential group whose focus was on the conditions of democracy and trust in government. (The Attorney General is sometimes asked to play that role in national security decision-making.) But if this isn't done or if the influence of the new group is in doubt (perhaps because public and political opinion is being powerfully shaped by fear of attacks), we might have to rely on new court decisions and new statutes to protect privacy. What such new law would look like is my subject.

---

[1] This story could as easily have been played out "down the hall in the same building" in another room where searches abroad of foreign individuals under another section of the Patriot Act have been considered by a group of officials – none of whom, however, bears the responsibility to represent concerns for U.S. foreign relations, alliances or diplomacy.

II. IS RAPIDLY INCREASING U.S. GOVERNMENT SURVEILLANCE OF ITS OWN CITIZENS A REAL CONCERN?

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, fears, actions, intentions, and associates. These multiple funds of information will also be readily subject to electronic search, storage, and combination and will generate generally reliable conclusions about our past activities and predictions about our future activities as individuals, as well as the same about the *networks* of individuals that each of us inhabits and populates.

A. THE LARGEST NEW SOURCES OF SURVEILLANCE

Using the "third party" platform to gather metadata under Section 215 of the Patriot Act – data about to whom each of us speaks by phone, when, and for how long – is a major step in that direction. That data, if fully exploited, would reveal most of our associates, and like a GPS device secretly placed on your car, many of our activities A second example is the developing technology for making and recording observations not previously possible from the platform of places open to the public and for identifying who is being observed, thus defeating anonymity. Surveillance by drones or street cameras or heat-detecting technologies would be illustrative.

In this Essay, I will use these two important new forms of surveillance regulated under old legal platforms as my examples of new technology narrowing traditional privacy. But there will be others; this Essay seeks general causes and useful ways to think about remedies.

Consider each of these two examples in turn. The Section 215 program presents a compelling illustration of a vast internet-based increase in both surveillance and the capacity for surveillance. For lack of agreement in Congress on a new legal structure, the National Security Agency is still collecting information (metadata) on a very high percentage of the total telephone calls of U.S. persons. This puts in the hands of the NSA massive information as to who are the associates and what are the business and relational transactions of each of hundreds of millions of Americans.

Then turn to the second illustrative category of innovations in surveillance. Our major cities as well as the federal government have learned to use digital collection of visual and other sensory data (*e.g.*, heat radiations and drug smells) that in earlier times, indeed since the country's beginning, have been imperceptible by people at a distance, or blocked by physical barriers, through which today government officials can sometimes now observe. Facial or license plate "recognition" programs will soon threaten the privacy benefits of anonymity on city streets or in sports stadiums or wherever crowds provide cover. Acts in

public that were previously unobserved or unnoticed or anonymous can now be observed, recorded, studied for purposes of prediction about individuals, and identified with a particular individual.

Another way of assessing the extent of the changes we should anticipate is to appraise the continuing reliability of the set of legal protections of our privacy against government surveillance. Defenders of the NSA program argue passionately that it is justified because it is legal. If so, what gaps in our laws permit and invite it?

Little has changed about either the power of the legal authority of government – or, more surprisingly, its practical capacity – to learn almost everything about someone it considers especially dangerous. By use of informants, undercover agents, and electronic surveillance, even a half-century ago investigators could capture immense amounts of private information about Jimmy Hoffa or Martin Luther King. And besides unchanged legal authority, surely privacy has long been protected by government's respect for custom and history and its fear of public outrage. These are still at work in our society. What, then, has changed?

What's changed is that the new surveillance enables vastly increased discovery within the old legal framework, defining what is "not-a-search," and forcing a choice between a great loss of privacy and significant changes in these rules. To limit the loss of privacy, we may need to abandon old understandings about what forms of surveillance do not constitute a search and thus are not subjected to the protective provisions of the Constitution and our privacy statutes.

B. IS *GOVERNMENT* SURVEILLANCE PARTICULARLY IMPORTANT?

Why should we care particularly about government surveillance in a world where private surveillance on the internet and the information and predictions that can be derived from a mass of such information are driving much of the economy of the internet as companies seek knowledge useful for developing and selling new products?

Government surveillance has far greater reach. FBI and other law enforcement agents can – without any need of a predicate or judicial warrant – do whatever private individuals are allowed to do to discover information, using one of the "not-a-search" exceptions. 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 – a standard much more far-reaching than probable cause or reasonable suspicion. 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. What private businesses can obtain by requiring a waiver of privacy rights as a condition of access to their goods or services, the government can also obtain without even that strained form of consent and without the alerting knowledge that consent gives to the individual being monitored.

The government is allowed to use informants and undercover agents in a way that is not available to businesses. The government can and does develop technology, such as drones, which can greatly increase its powers to observe the activities of individuals. All of this can be done without any special showing of need and without getting a judge's certificate that a required predicate such as "probable cause" is met. With a predicate and a judicial warrant, the government can search places or activities, such as 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 seeking to make you a loyal customer. It can turn suspicions into investigations, arrest and search with probable cause; it can deny appointments or other discretionary benefits, insist on cumbersome formalities when you cross U.S. borders, and influence the actions of others by making obvious its suspicion of, or attention to, particular individuals. It can store data to be used for any of these purposes or for noncriminal forms of regulation.

The special powers of the government to obtain information and the special dangers to individuals associated with discretionary uses of that information go far to explain why we have a 4th and a 5th Amendment in the Bill of Rights. The history of the 4th and 5th Amendments is a history of enduring fears of governmental surveillance.

C. The Independent Significance of Fear of Loss of Privacy to Secret Governmental Surveillance

The capacity to collect, process, and use massive amounts of information on great numbers of citizens does not necessarily mean that the information is actually used in a way threatening to a citizen's privacy. Phone metadata, images from street cameras, and the product of a secretly placed global positioning device, could simply be stored until some form of predicate, such as probable cause, gave reason to pull it out of the inventory for view and study. And perhaps I need not worry about cameras or global positioning devices or cell phones collecting information on where I have been and what I have done, so long as there must be probable cause or some lesser predicate (e.g., "reasonable suspicion") for the government to access what it has collected.

In fact, on this theory, a huge inventory of government metadata on phone use is stored by the NSA where it is readily available to be searched – but only on an internal governmental determination of "reasonable suspicion" that it involves a terrorist plan. The inventory may not be searched without that internal determination. So, in both examples I have chosen, concern about adverse effects of lost privacy turns on the effect on citizens' attitudes and behavior of knowing that records of what they are doing will be held by the government and could, perhaps improperly, be viewed at a later date without a judicial warrant -- with no

more than a bureaucratic determination of "reasonable suspicion" that the record bears on a national security threat.

The presence of fear, even unreasonable fear, has important effects on the confident and free social and political life on which democracy depends. Fear of discovery alone could easily affect with whom I associate, for example, or what use I make of psychiatrists or drugs. The fear is far deeper and more lasting if a warrant from a judge is not required. Internal agency processes are not an adequate substitute. The deep suspicions that are valuable in an agency charged with preventing terrorism or preventing crime have a dark side; they will infect its judgment of when there is a genuine need to see the required information. Important consequences turn on the citizens' trust that data the government has acquired will not be used without there being a "real" need for its use. Much of the population would not trust any such assurance by the NSA or the FBI alone.

Perceptions of government prying do matter. Whether a dramatic growth in the capacity for, and fruits of, government surveillance would be experienced as harmful to individual freedom, civil society and democratic institutions depend on more than how the information would, in fact, be used. Fear also depends on what other potential uses citizens would suspect; the exercise of individual liberty and autonomy additionally depend on what citizens suspect might happen with that information and the precautionary steps – curtailment of entirely lawful activities, for example – citizens might take. Attitudes toward government and one's freedoms also depend upon a number of broader contextual factors: the extent of the perceived danger sought to be prevented; the current level of suspicion or trust in the government; the history and culture of privacy in the society; and much else. Some few would argue that the loss of privacy might not be a concern at all. After all, most people do not harbor a crime or a scandal that they must hide behind claims to privacy; their lives are too proper for that. But those voices are a small minority; for most people, the value of privacy is to protect the possibility of association and, particularly, intimacy with others, irrespective of whether one has anything to hide in the way of crime or scandal.

One fact is clear. The fear and the prospect of rapidly expanding government surveillance in the United States are plainly there on the near-horizon. The children of the Snowden age take it for granted that they are being monitored and they fear the social effects of that monitoring.

D. What Is Causing the New Burst of Surveillance?

So we are moving rapidly in the direction of social changes that we may not want. It might be wise to halt long enough to ask, "What forces are pushing such changes forward?"

Many would say that the changes we have seen were simply signs of the temporary advance of surveillance as a policy choice to deal with the hopefully receding, temporary danger from jihadist terrorism. (That explanation is illustrated by the story in the Introduction.) Isn't that why the Bush and Obama

administrations wanted so much information from the records of our phone calls? The threat might be revived by the appearance of ISIS but still not outlast an age of jihadist terrorism. On the other hand, what we are seeing may be the result of the opportunities presented by new, business-driven, computer-based ease of collecting even tidbits of information that, once combined, "might" be useful for security or law enforcement or political purposes.

The business demand for masses of information relevant to product designs and sales has in fact pushed much of the advance in technology for internet surveillance; perhaps the availability of the product of such surveillance is what has created a government appetite for information about the activities of its citizens and residents. If so, the causes of and remedies for lost privacy might depend on regulating the terms of the government demanding (or even merely requesting) the information produced and stored by the business world (use of the "third party" platform) – a road already taken in one important privacy statute, the Stored Communications Act.

III. A Remedy Modeled on the 4th Amendment

The 4th Amendment prescribes a showing to a judge that a search in private places or of private communications or of private records is justified by the prospect of finding evidence relevant to a comparatively compelling government need, such as to solve a crime or prevent a severe danger. Knowledge of his innocence – of the absence of evidence to be found – provides substantial assurance to any individual who would otherwise be fearful for his privacy. But this assurance is not available if the government is using as a platform for surveillance one of the activities not covered by the 4th or 5th Amendments – activities that are "not a search" or "not self-incrimination". The government has far more capacity, far wider interest, and far more threatening powers to obtain information from these "not-a-search" areas.

A. A Second Form of Protection of Citizens' Privacy

Privacy against government surveillance is protected in two distinct ways. (1) Privacy-protecting law, reflecting history and custom, is a creature of constitutional and statutory policy. A requirement of a predicate for surveillance limits when and where a search in a private place or of private communications can take place. (2) But there is another form of privacy that is at least equally important and applicable to places that have no legally established privacy protections. This second type of privacy allows individuals to take advantage of the facts of the physical world and the laws of nature – or, in the case of "Big Data," the limits of human administrative capacities – to hide what they want to keep secret, by using the privacy furnished by physical cover or distance; or

alternatively by the infeasibility and burdens of creating or demanding, and then having to hold and process, massive files.

This second form of privacy from government is rapidly narrowing, however. It is not that the law has changed. Officials have long been entitled to observe what is in plain view from a public location. What has changed dramatically is what can now 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, 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 sees what the inattention of a human viewer might have caused to be overlooked and modern surveillance remembers and archives what might otherwise have been forgotten.

Members of the public are legally entitled to occupy airspace 50,000 feet above the ground, but they can't get there and, in any case, little can be seen from that height without very advanced and expensive technology. Government can do both. Similarly, government officials have always been free to demand records relevant to a grand jury's interests. Yet the difficulties of knowing who has what records; of trusting the recipient of a subpoena to produce the appropriate records; of collecting them and retaining them safely; of searching the records and of combining the records with other information in order to discover (or make predictions about) an individual's activity were all far too costly and cumbersome to be routine before the age of the advanced computer.

In both cases nature has provided, as a practical matter – before the age of Big Data – an important opportunity and mechanism for privacy, without the need of rules about what is a private place with respect to a "search." It is in this area of "natural" privacy -- either in places or in communications or in records of one's transactions or activities with respect to which other private individuals have been allowed but are disallowed from gathering information – that new government technology using the old legal authority can now observe and preserve vast quantities of data. No new law has been necessary to grant immense new capacities for surveillance in the areas of such "natural protection." Yet no new powers needed to be granted in these areas.

Consider the latter point first. For decades, the government has been able to demand records about their customers from business third parties without a predicate or warrant. Borrowing from still older legal rules based on the concepts of constructive consent and assumption of risk – associated with, for example, foolishly trusting a false friend or trusting someone who turned out to be a government informant with records or other information – the Supreme Court has held that any records of transactions with a third party are subject to government demands for access from that third party. The government has not been constrained in any significant way in its power to subpoena records, papers, or physical objects. It has been able to search for, seize, retain, and use records pertaining to a target of a search, but did not belong to that target. Finally, it has

been able to exploit the fear of further investigation or mistakes about the reach of actual government authority in order to obtain consent to what otherwise would have required a predicate and approval by a court.

The result is this: Whether in the form of gathering, storing, combining, and exploiting data, or in the form of new sensor devices that can penetrate areas that used to be protected by an individual taking advantage of the laws of nature and storing the results digitally, the new government surveillance as it stands today needs no new legal powers in most cases to proceed without a predicate or warrant.

Nor is the degree of cumulative surveillance of a suspect's life much changed. Though at a much greater cost per suspect, the government has long been able to use a trusted informant (such as Partin, who spied on Jimmy Hoffa) to gather a very large amount of information about a targeted individual. The information it could obtain about a suspect was sometimes as great as the information that so troubled today's Supreme Court in the case of an electronic GPS device (*Jones*) or the information stored on a cell phone, seized "incident to an arrest" (*Riley v. California*).

Indeed, the government's ability to amass a great amount of information about a particular individual being targeted – to assemble, analyze, and combine it with other information – has long been possible in particular cases. What is new is that these steps can now be taken cheaply and quickly by the use of a global positioning device or the seizure of a mobile phone for one or any number of individuals. These surveillance methods can be made applicable to much of the U.S. population through demands for metadata, collected for other purposes by businesses, such as Verizon or Google.

The situation today is thus not a consequence of any great change in the legal powers of the government to engage in surveillance. It results instead from a massive change in technologies to exploit surveillance in areas that the law has not protected in the past – allowing massive discovery of information, yet without violating the law. This has created a new situation where citizens have much more reason to be concerned about their privacy and the effects of loss of privacy: an increase in the practical consequences of disagreeing with government and an increase in the social pressure to conform one's behavior.

The causes of the vast increase in surveillance has been, in part, a vast increase in the felt need for such surveillance to deal with post – 9/11 terrorism and, in part, the natural human desire of investigators to exploit emerging technology that can operate in the areas where the law has not granted protection. The FBI, the CIA, and the NSA (among others) have major research arms to explore the uses of new technologies; they also have access to the product of new technologies developed by internet-based businesses.

In fact, both causes intertwine. The NSA seems determined to get access to all the business information it can through the §215 program, although that effort has apparently facilitated, at most, a single occasion that may have reduced the threat of terrorism. The only constraints on the NSA program are costs

(which are manageable) and public resentment (which depends on learning of a highly secret program). Many types of information could conceivably be useful enough to bear the marginal cost of acquisition and storage if that cost is small enough. Secrecy blocks the other cost: anger by those who learn of their vulnerability to the new program.

B. THE REMARKABLE 4TH AMENDMENT

When committees of the House and Senate have addressed questions presented by the NSA program of collecting masses of metadata about the phone calls of almost every American, the recommended solution in each committee has involved defining and limiting the search terms that could be used in making requests from the phone service providers. It would have been far wiser for either the Congress or the Supreme Court to turn to the 4th Amendment and adjust the outdated interpretations which allow modern, highly sophisticated surveillance (in situations where these doctrines apply) to define surveillance that today remains free of 4th Amendment requirements. That, as we shall see, is the path the Supreme Court is on.

The way the 4th Amendment works is straightforward; comprehensible to Americans who would distrust a secret reliance merely on search terms; and surprisingly useful. To search any place, record, or communication which is not freed, by Supreme Court doctrine, of the 4th Amendment obligations of probable cause and a warrant to search any place, record, or communication which is not excepted by Supreme Court doctrine from 4th Amendment obligations of a probable cause and a warrant (with some exceptions) requires a factual basis for thinking it probable (or, in some cases, by 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 and authorize a search or electronic surveillance and specify the conditions under which it may take place.

The attributes and advantages of this system are immense. Consider six wonders of the 4th Amendment:

> (1) The system is entirely comprehensible and makes perfect sense to a very high percentage of Americans who would never understand or trust the neutrality of government officials furnishing secret search terms to technicians at the NSA.
>
> (2) The way it works makes unnecessary any substantial effort to establish that the costs in terms of privacy of a particular search are less than benefits to law enforcement or national security. It does not require an extraordinarily complicated balancing of the amount of damage a search does to privacy versus the amount of value it adds in terms of reduced crime or reduced danger to national security. While we would

like to allow only those searches whose cost in terms of citizen insecurity are outweighed by the benefits in terms of solving or preventing a crime, the cost of making that judgment in the case of each individual search would be immense.

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 fears of government misuse of the power to search and that itself 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 was the location 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 is the activity 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 cost and benefits of a particular case is replaced under the 4th Amendment by simply requiring a showing that evidence of a crime or of a grave future threat would be found in the 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. 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 4th Amendment.

(3) Use of 4th Amendment standards provides assurance of privacy to the vast majority of citizens who are likely to know whether there is probable cause to search their places or surveil 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 4th Amendment, unlike a grand jury subpoena for documents, does not tip off the suspect that he is about to be searched (and thus should hide or destroy any evidence). The suspect takes no part in the decision of the court to issue a warrant.

(6) The 4th 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.

C. What About the 4th Amendment Has Allowed a Massive Increase in Surveillance?

As we have seen, the threat of new surveillance arises from a combination of remarkable new technology for surveillance and a "free pass" on having to satisfy a court as to the existence of a predicate and the conditions under which surveillance will take place. The "pass" comes in the form of established doctrine that excludes from the requirements of the 4th Amendment any search or electronic surveillance done with the consent of the suspect, any surveillance from a place where the public can be observed or overheard, any surveillance at a border crossing, any surveillance necessary for the protection of an officer and to prevent the destruction of evidence incident to an arrest, etc. The dual justifications for these exceptions to the 4th Amendment requirements are their relative lack of intrusiveness (*i.e.,* the absence of a clearly "reasonable expectation of privacy" – combined with the efficiency benefits of limiting the number of times a surveillance requires going through the judicial processes of the 4th Amendment.

In the situations I have just listed as embodying excuses from compliance with the 4th Amendment, time and energy could 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 only by the savings to the government in cost and time derived from bypassing the 4th Amendment. The "consent" rationale that justified the use of pen registers in the *Smith* case and the companion rationale of "assumption of the risk" in the *Hoffa* case are simply not true with regard to the records kept electronically by Verizon, Google, Facebook, and many others. An argument that the individual has 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, e.g., the "terms of service" of online companies) is produced by the business using it; it is rarely read; and there is little realistic option in the modern world for opting out even if it had been read.

The exception to the 4th 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. It makes little sense when sophisticated thermal-detection equipment can tell what is going on inside a home he 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 said between individuals can be detected in ways that the suspect cannot anticipate.

The *Robinson* case held that the protection of the officer making an arrest and the importance of preventing destruction of evidence by the suspect were too difficult to appraise in the heat of making an arrest. Therefore the very limited privacy of a gun or knife, or of stolen property, did not justify even the limited risks of a rule requiring an officer to have at least a reasonable suspicion of destroyable evidence or a weapon to justify searching a suspect incident to his arrest. But the privacy cost of allowing a smart phone to be searched incident to any arrest makes the situation very different. A similar argument applies to border searches. The cost in privacy is orders of magnitude greater.

Nor would the burdens on police, prosecutors, and courts be greatly increased by carefully narrowing outdated rules for what is "not-a-search". The requirement of a warrant to 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 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 search of a cell phone at the time of arrest or a border crossing could, as with the doctrines of consent to observations made from a public place, be set aside and a return made to the 4th Amendment's broader notions of probable cause and judicial certification of that finding. In short, the justifications for the "not-a-search" doctrine 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.

D. How has the Supreme Court responded to these changes?

The developments described above have not escaped 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 without high technology from a place open to the public is not a search.
    * But there is a search if the government uses sense-enhancing technology, not otherwise in general use, to discover information regarding the interior of a home or its curtilege that could not otherwise have been obtained without a trespass (*Kyllo*).

2. Use of a sophisticated method of surveillance that is only capable of detecting contraband is not a search. (*Place*)
    * But applying it to a house is a search (*Jardine*)

3. Taking advantage of consent granted for other purposes to engage in surveillance is not a search (*Hoffa, White*).

* But it is a search if it applies to a house (*Jardine*)

4. Using technology to gather information formerly obtainable without trespass by a conventional surveillance technique is not a search (Karo).

* But it is a search if the technology produces vastly more useable evidence (*Jones, Riley*).

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 (*Greenwood*).

* But it could be a search if what is disregarded is the possibility of high technology surveillance (*Dow Chemical*)

IV. The Remaining Questions

In short, we have a set of concepts defining what is not a search at all – a set that is no longer realistic, however. We have a technology that today is 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 4th 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 use of the "no search" categories in connection with sophisticated surveillance technology, which is frequently defined as technology too expensive or too rare to be available to most of the public. The cost of requiring a warrant under the 4th Amendment is, at most, delay and much of the delay can be prevented with an emergency exception such as that which the Electronic Surveillance statutes embody.

The path ahead seems clear: follow the lead that the Supreme Court has begun to mark by narrowing the "not-a-search" categories. That will leave only a few unanswered questions.

A. The Required Predicate

We need to specify what the government must show to obtain a warrant in these new areas. Two situations present different variations of such a predicate – a showing of need for either (1) information relevant to a crime such as the Fourth Amendment requires or (2) a showing of a foreign threat like those dealt with by the Foreign Intelligence Surveillance Act. In either case the required probability

that the evidence will be found in a particular place, communication, or set of documents and will be helpful to the investigation could be "probable cause" or the lesser standard of "reasonable suspicion." In either case, judicial ratification of that predicate (i.e., a warrant) could be required, except for emergencies. The most serious difficulty arises elsewhere.

If a predicate and a warrant are to be required for the government to order a search and seizure of voluminous business records for information about transactions relevant to (1) or (2) above, the search may be for records about a named individual. Alternatively, it could be for names or other identifying information about whoever has engaged in or has been associated with a specified activity, purchase, location, relationship, etc. over a particular period. In a traditional police investigation, for example, such information might be used to narrow the field of potential suspects to those at the scene of the crime and might then be combined with other available "narrowing" data (*e.g.*, a list of gun purchasers) to identify the likely perpetrator; or intelligence agencies might use such information to identify members of dangerous foreign groups or organizations.

It is easy to imagine the predicate for the first category: either probable cause or reasonable suspicion that evidence useful to dealing with a serious crime or threat is likely to be found in a particular place or communication, or a set of records (if the "no search" rule for information entrusted to a third party is abandoned). But defining the requirement for the second category is far more difficult.

If the government obtains access to records revealing those who are openly engaged in a particular activity; or who live or work openly in a particular place; or who associate, communicate, or deal frequently and publicly with each other, the data it obtains has never been guarded from others' eyes or ears. Nor is it likely to involve intimate materials (like medical records, or a record of internet searches, or records of other viewing or reading interests, or a view into a place as private as a home). Why should anyone be able to object to the government obtaining and holding such nearly public group statistics?

"Big data" technology has greatly increased our capacity to draw conclusions from collections of near-public data such as these – to discover what characteristics of several collections, if combined appropriately, are predictive of the future or revealing of a role in a past event. The techniques of big data analysis may well reveal very personal and sensitive information about the prior or future activities of a readily identifiable individual.

We need a check on this – but not a prohibition. Allowing the government to collect and process such information may turn out to be extremely useful in protecting our security and moreover not invasive of the privacy of most members of the group that the data describes. So we need a middle ground between an unchecked power to search, to be followed by analysis with other data, on the one hand, and a flat denial of access to such data held by third parties, on the other. We need a different type of predicate that would provide

some of the privacy protections of a warrant in these situations of reduced privacy, while still allowing the use of Big Data processing to develop information and conclusions useful to our security.

We thus need a middle ground. If our privacy is to be protected against searches and analyzing processing of third-party records, it must be by rules that don't require a warrant particularly describing the things to be seized. At the time a data file is obtained, we often won't know what about it is likely to be revealing. If the government's use of big data is to contribute to our safety, the predicate for the legal authorization granted by a warrant should be a showing of a serious need for using techniques of big data analysis to draw conclusions about individuals and private matters from previously collected fields of data – *not* what information about the activities of a particular suspect we expect to find.

B. Model Statutory Language

The plausible middle ground is that the government must, and should be able to, seek a warrant to obtain non-private information that can be used to predict or identify private information about individuals. As an example, consider a possible statute with the following provisions:

> *(i) To obtain a warrant [under this section] the government must provide specific and articulable facts showing reason to believe that any data sought under this provision will, if analyzed in specified ways and in connection with other specified data files, be likely to provide significant assistance in an ongoing investigation either of a felony committed under federal or state laws or of a particular, identified foreign threat. The court may grant access to sharply limited data without such a showing only if the government satisfies the court that only with such access to information to be used for discovering and testing correlations can it satisfy the standard set forth above.*
>
> *(ii) The court shall not grant access to more data than is shown to be necessary for these purposes. If in the course of this or another investigation the data made available to the government under this section is to be used with other techniques and/or other data files or in a different ongoing investigation, a new warrant must be obtained for such new uses of the previously acquired data.*
>
> *(iii) Any warrant obtained under this provision shall provide for the prompt destruction of any information obtained under the warrant if it is not relevant to the investigative purposes for which the warrant was issued – other than information concerning a different felony or a different foreign threat. Any data files obtained under the warrant and any copies thereof will be destroyed within three years of acquisition unless a new warrant is obtained.*

C. Remaining Questions

(1) Should even a warrant, based on probable cause, permit the vast expansion of surveillance that new technology allows? Our privacy will still be reduced by new technology, although only when the government has probable cause to believe that with the help of new technology it can find evidence of a crime or a grave national security threat. The idea of permitting an increase in surveillance and a parallel reduction in privacy despite applying the fundamental procedures of the 4th Amendment seems a reasonable price to pay to avoid the confusion of trying to limit even a search with a warrant by the adoption of a new restriction limiting discovery to what, hypothetically, could have been discovered prior to the development of new technology.

(2) Should a warrant be required *before* using any new, technologically advanced form of surveillance not generally available to the public? Or should a warrant only be required when the collected information is read? What if the government is prepared to use new capacities of technology just to acquire and store vast amounts of un-read information? Should it be permitted to do that without a predicate or judicial approval (a warrant) *until* the stored information will be searched in a traditional way, at which time a predicate and warrant would be required? The latter is the process now being used by the NSA with regard to telephone meta-records.

On the one hand, there is no loss of privacy or of the 4th Amendment's protections if information is never seen by the government until after a warrant has been obtained; and the government's possession of the records may make it possible to search them far more quickly in the event of an emergency. On the other, transparency at the stage of acquiring data provides a sense of confidence in privacy that government storage of records obtained without compliance with the 4th Amendment will never create. Much would favor requiring a warrant when the information or records is obtained and taking other measures to speed compliance.

(3) Should any new rules for business records – narrowing or eliminating the third party doctrine – apply to a judicial subpoena as well as to a search? A subpoena could be used without probable cause to obtain the same records as could, under the proposal, be obtained by a search only after compliance with a warrant requiring probable cause or another predicate. Indeed, it is becoming far more difficult to destroy electronic evidence, eliminating one prior deterrent to use of a subpoena in place of a search. Therefore, so much of the privacy preserved (by imposing a warrant requirement on technology-exploiting platforms which were previously "not-a-search") would be promptly lost to a practice of substituting the use of subpoenas for physical searches of digitized records that it would be wise to require similar protections for searches of records by subpoenas.

(4) What should we do about the fact that as the availability of private technology capable of dramatic new forms of surveillance spreads, the extent of citizen privacy is likely to narrow? If the Supreme Court comes to require a

warrant only when high technology available to the government allows far more surveillance than private citizens have available to them – won't government surveillance without a requirement of probable cause expand as a consequence of predictable growth of private access to surveillance technologies, as those technologies become cheaper and more widespread?

Statutes could forbid anyone – private individuals as well as governments – from engaging in certain forms of surveillance of their neighbors. We do that now with regard to electronic surveillance of phones. This would prevent the area of privacy from continuing to narrow as it appears that it might do, even with a warrant requirement like the one the Supreme Court seems to be gradually adopting.

V. Conclusion

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

- 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 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 4th Amendment. The first is very dangerous to our freedoms; the second is unlikely so long as we face international and domestic dangers.

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, *i.e.*, of honoring reasonable expectations of privacy. These doctrines provide unregulated and unrestricted platforms – *e.g.*, views from public places, records made and held by businesses or other associates, searches incident to an arrest, uninformed consent, etc. – for enabling 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 for them.

That direction, if adopted in legislation as well as in court opinions, 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 – indeed,

one that may prove necessary in light of the Second Circuit's opinion of May 7, 2015 in *ACLU v. Clapper*.

*

(Editor's note: This Lawfare Research Paper draft of May 10, 2015 will be updated to reflect additional copy editing, notes, and possibly further discussion of several remaining issues.)