THE FUTURE OF THE CONSTITUTION

April 19, 2011

Paul Edmondson - People boarding DC metro commuter train in terminal.

Use Restrictions and the Future of Surveillance Law

Orin S. Kerr

Governance Studies at BROOKINGS

INTRODUCTION

The year 2030 was the year of the subway terror attack threat. As far back as the 2004 Madrid subway bombing, terrorists had seen how a single modest subway attack could wreak havoc on a busy city center. Sporadic attacks continued in the first three decades of the 21st century, including unsuccessful attacks on the New York subway in 2018 and the Washington, DC, Metro system in 2023.

But 2030 changed everything. On January 1, 2030, Abdullah Omar, the leader of the Brotherhood, the reincarnation of the earlier Al Qaeda network, made an ominous announcement.

Orin S. Kerr is a professor of law at the George Washington University Law School.

The Brotherhood had a dozen sleeper cells in the United States, Omar announced. In 2030, he would activate the cells. The cells would launch terror attacks on the transit systems of each of five major cities. Each system would be hit twice, and a few would be hit more. Omar threatened that each attack would come with a "surprise."

Omar named the transit systems: The New York City Subway, the Washington Metro, the Chicago "L," the San Francisco BART system, and the Boston "T." Each system would be attacked during the year unless the United States agreed to withdraw all support from the state of Israel.

Some critics dismissed the threat as posturing. Others doubted the Brotherhood could pull it off.

But in classified briefings, the Director of National Intelligence told President Booker that he thought the threat was extremely real. Omar's promised "surprise" was likely some kind of biological attack. Some attacks might fail. But others could work. The overall damage to life and to the economy amounted to a grave national threat, he explained, and the threat demanded a thorough response.

President Booker agreed. He set up a Commission to advise him on how to respond. The Commission, consisting of top intelligence and national security officials, recommended establishing a new federal surveillance system. The system would be known formally as the "Minding Our National-Interest Transit or Rail" program. It would be known informally by its acronym: MONITOR.

MONITOR worked by requiring all subway passengers to use a MONITOR card when they entered subway systems. Each card was activated by its owner's fingerprints. The fingerprints identified the user and kept records of where the user had entered and where the user existed the system.

The Department of Homeland Security administered the MONITOR system out of a central office in downtown Washington, DC. MONITOR's computers kept records of every entry into and exit from the subway, and that information would be fed into the government's database in its central office.

The system assigned each subway rider one of three colors. The first color was green, which meant that the rider was authorized to ride the subway. The second color was yellow, which meant that the user was a "person of interest" that the

government wanted to follow (such as someone on a terrorist watchlist). Yellow riders were allowed to enter the subway, but their progress was flagged by the MONITOR computers. The third color was red. Riders assigned red were not allowed to enter the subway system at all.

MONITOR was up and running by late February, and it ran through the end of the year. By most accounts, it was a mixed success. Its most celebrated use was identifying a terror cell known as the "South Loop Seven."

The South Loop Seven was a group of seven young Muslim men who attempted to enter the Chicago "L" system within minutes of each other. Four of the seven men had been flagged as yellow because they were on a terrorist watch list. The entrance of all four yellow-marked riders into the same station in a short period triggered an immediate response from Homeland Security.

The four men were found minutes later with bomb-related materials in knapsacks. The "L" trains were shut down immediately. A search of the station yielded the three other cell members, each of whom also had bomb materials in packages he was carrying.

To many observers, MONITOR's success in stopping the South Loop Seven justified the entire program. But other uses of MONITOR proved more controversial.

For example, MONITOR's access to a fingerprint database drew the attention of the FBI. The FBI sought to use the fingerprint database to crack unsolved crimes. MONITOR had not been intended to be used for criminal investigations, but President Booker eventually allowed MONITOR's data to be provided to the FBI with the proviso that it be used to solve only serious crimes. Hundreds of crimes were solved. Some of those crimes were serious, including murder and rape. Others were decidedly less serious, ranging from mail fraud to tax evasion.

Abuses occurred, as well. For example, a few employees of the Department of Homeland Security were caught using MONITOR for personal reasons. One employee used the data to keep tabs on his wife, whom he suspected of having an affair. The employee flagged his wife's account yellow so he could watch her coming and going through the DC metro system.

In another case, an employee of Homeland Security lost a laptop computer that included a MONITOR database containing millions of datasets of fingerprints. The computer was never recovered. No one knows if it was destroyed, or if the information eventually made it into the hands of criminals or even foreign governments.

The Lessons of MONITOR

What are the lessons of MONITOR? In my view, MONITOR calls for a shift in our thinking about surveillance. In the past, the law has tried to regulate surveillance mostly by focusing on whether data can be created. The focus has been on the first stage of surveillance systems, the collection of data.

That must change. Computer surveillance uses widespread collection and analysis of less intrusive information to yield clues normally observable only through the collection of more intrusive information. To achieve those benefits, the law will need to allow relatively widespread collection of data but then give greater emphasis and attention to its use and disclosure.

In short, the future of surveillance calls for a shift in the legal system's focus not merely a shift in *how* to regulate but a shift was well in *what* to regulate. Instead of focusing solely on the initial collection of information, we need to distribute regulation along the entire spectrum of the surveillance process. The future of surveillance is a future of use restrictions — rules that strictly regulate what the government can do with information it has collected and processed.

Of course, the law should still regulate the collection of evidence. But surveillance law shouldn't end there. The shift to computerization requires renewed attention on regulating the use and disclosure of information, not just its collection. To see why, we need to understand the computerization shift and the stages of surveillance law. We can then see how use restrictions would be the key to protecting privacy while ensuring security in the case of the MONITOR system.

The Computerization Shift

In the past, information ordinarily was collected and shared using the human senses. We generally knew what we knew because we had either seen it directly or heard it from someone else. Knowledge was based entirely on personal observation. If you wanted to know what was happening, you had to go out and take a look. You had to see what was happening and observe it with your own eyes, or at least speak to those who had done so to get a second-hand account. The human senses regulated everything.

In that world, surveillance systems were simple. The "system" was really just a person. The person would listen or watch. If he saw something notable, he would tell others about it.

Computers change everything. More and more, our daily lives are assisted by and occur through computers. Computer networks are extraordinary tools for doing remotely what we used to have to do in person. We wake up in the morning, and use the network to send and receive messages. We make our purchases online, using the network to select and order goods. Instead of hiring a person to watch our property, we use cameras to record what goes on in open places and to keep records of what occurred. All of these routine steps are facilitated by computers

and computer networks.

The switch from people to computers means that knowing what's happening requires collecting and analyzing data from the networks themselves. The network contains information zipping around the world, and the only way to know what is happening is to analyze it. Specifically, some device must collect the information, and some device must manipulate it. The information must then go from the computer to a person, and in some cases, from a person to the public. The result is a substitution effect: Work that used to be done entirely by the human senses now must be done in part by tools.

The shift to computerization complicates the process of surveillance. In a world of human surveillance, a system of surveillance was one step: The human would observe the information and then disclose it to others. Computers add a few steps in the process in a critical way. Instead, of one step, there are now four steps: Computer collection, computer processing, human disclosure, and public disclosure. To see how computers change the way the law should regulate surveillance, we need to focus on those four steps.

The Four Stages of Computer Surveillance

The shift to computerization has profound consequences for how we think about surveillance law. There are now four basic stages of computer-based surveillance systems: 1) data collection, 2) data manipulation by a machine, 3) human disclosure, and 4) public disclosure. A threshold problem faced by any system of surveillance law is which of these steps – or which combination of them – should be the focal points of legal regulation. For example, should the law focus on regulating the initial collection of information, leaving the downstream questions of processing and use unregulated? Alternatively, should the law allow broad initial collection, and then more carefully restrict human access or eventual use and disclosure?

Evidence Collection

The first stage of any government surveillance program is evidence collection. The idea here is simple; surveillance requires access to and copying of information. Evidence collection can occur in many different ways. It may occur through use of a device such as a "bug" or a wiretapping program. Alternatively, the government may obtain a copy of data collected elsewhere such as from a private third-party provider. The evidence may be stored in any form. Although electronic forms are most common today, it could be on paper or on a magnetic tape or some other mechanism. In all of these cases, the government comes into possession of its own copy of the information.

The rationale for regulating evidence collection is obvious: The government cannot misuse evidence if it does not have it in the first place. Conversely, permitting evidence collection and only regulating subsequent use or disclosure

can permit governmental abuses.

Data Manipulation by Machine

Data manipulation by a machine provides the next stage of surveillance systems. At this stage, the government has the data in its possession, and it now wants to manipulate the information to achieve particular goals. Perhaps the government wants to aggregate the information into a database. Perhaps the government wants to aggregate the information and then "mine" the data for trends or clues that might signal a likelihood of criminal or terrorist activity.

Or perhaps the government wants to combine two databases, adding information developed for one agency or one reason with information developed for another agency or reason. Whatever the goals, we can assume at this stage that no human being accesses the information or the results of any analysis of it. The collected information exists but is not viewed by any person.

Disclosure to a Person inside the Program

The third stage of a surveillance system is disclosure to a person who is a part of the surveillance program. At this stage, an individual with proper access to the database receives the fruits of the data collection and manipulation.

For example, an IRS employee tasked with reviewing tax information may enter queries into a database of tax filings. A police officer who has just pulled over a driver for speeding may query a database of driving records to determine if the driver has received speeding tickets in the past. A keyword search through a database of seized e-mails may reveal positive "hits" where the keyword appeared. In all of these cases, information from or about the database is disclosed to a government employee with proper access rights to the database.

This stage of surveillance systems raises privacy concerns because it involves human access to sensitive information, and human access is a necessary step to abuse. Unlike stage two, data manipulation, stage three envisions giving government employees access to often very private data. Access creates the possibility of abuse, triggering privacy concerns beyond stage two.

Public Disclosure

The fourth and final stage is disclosure outside the government. At this stage, the information collected and analyzed by the government is actually disclosed or used outside the agency.

For example, the government might seek to use the fruits of wiretapping in a criminal case, and therefore might disclose the private phone calls in open court for the jury to see. A government insider might seek to embarrass someone else, and might leak private information about that person from a government database to the press. In some cases, the government will disclose the information pursuant

to a formal request, such as a request under the Freedom of Information Act. In all of these examples, information collected by the government is disclosed to members of the public.

Outside disclosure can occur in different forms. In some cases, the disclosure will be direct: a government official with control over information will communicate the information explicitly, authenticating the information disclosed. This would be the case when the government seeks to disclose the fruits of wiretapping for use in a criminal case.

In many cases, however, the disclosure will be indirect. If government data-mining of collected call records leads officials to determine that they have identified a terrorist cell, they might respond by sweeping in and arresting the members of the cell. The fact of the arrest does not actually disclose the data collected or metadata obtained: however, the arrests might be used to help piece together the government's surveillance. The information isn't disclosed, but actions based on the information may be public and in some cases will resemble a direct disclosure in substance if not in form.

The Old Law of Surveillance

In the past, the law of surveillance has focused primarily on the first stage of surveillance systems, the initial collection of evidence. The Fourth Amendment's prohibition on unreasonable searches and seizures regulates access to information, not downstream use. If the government comes across information legally, then it is free to use that information however officials would like.

The reasons for this focus are largely historical. The Fourth Amendment was enacted to limit the government's ability to break into homes and other private spaces in order to take away private property. Breaking into the home was a search. Taking away property was a seizure. As a result, the Fourth Amendment was designed to focus on the initial invasion of privacy – the initial entrance into private spaces – and the retrieval of what the government observed. Once property or information is exposed and retrieved, the work of the Fourth Amendment is done.

The statutory Wiretap Act has a similar focus. The Wiretap Act's most important prohibition is the "intercept" of data without a warrant or an applicable exception. Intercept is defined as "acquisition" of the contents of the data, which means that the Wiretap Act regulates the initial stage of evidence collection. Surveillance laws such as the Stored Communications Act also monitor the initial government acquisition of data; the laws focus on regulating when the government can obtain data, rather than what the government does once the information has been obtained.

In contrast, the later stages have received little attention by privacy laws. The law mostly focuses on the collection of evidence: Relatively little attention is placed on what happens afterwards.

Exceptions exist. For example, information in tax returns filed with the IRS generally stays with the IRS; the FBI is not normally given access to that information for criminal investigations. Similarly, information obtained by a grand jury pursuant to grand jury authorities can only be disclosed within the government to those working on the criminal investigation. The basic idea is that the government is a "they" not an "it," and limiting data sharing is essentially the same as limiting data collection for individual groups and institutions with different roles within the government.

But these laws are the exception, not the rule. For the most part, the law of surveillance has focused on how evidence is collected, rather than how it has been processed, used, and disclosed.

The Case for Use Restrictions

The new forms of computer surveillance should change that. The benefits of computer surveillance is that they can process information quickly and inexpensively to learn what would have been unknowable. Assembling and processing information may lead to plausible conclusions that are far more far-reaching than the information left separate. If so, data manipulation can have an amplifying effect, turning low impact information in isolation into high impact information when processed.

Reaping these benefits requires surveillance systems that allow the initial collection and processing. To reap those benefits, the best way to design surveillance systems is to allow the initial collection but then place sharp limits on the later stages such as disclosure.

Of course, choosing where to regulate requires balancing competing concerns in minimizing disclosure risks and maximizing the effectiveness of the surveillance system. The proper balance will depend on the interests involved. A database designed to identify terrorists will have a very different government interest from a database designed to identify suspects likely to possess marijuana. A database containing the contents of phone calls is very different from a database containing only the numbers dialed without the contents. Given the diversity of interests and privacy concerns, it is clear that different surveillance regimes will use different regulatory points in different proportions.

As a general rule, however, the shift to electronic surveillance systems requires a shift in emphasis from regulating the early stages of surveillance to regulating the later stages of surveillance.

In a traditional surveillance system, such as those before the advent of computers, the primary legal regulation sensibly focused on the early stages of surveillance. The shift to computerized systems and the future of low-cost surveillance methods will shift the emphasis to the later stages, and in particular the final stage of public disclosure.

The advantages of computer surveillance follow from their ability to yield

important information through widespread collection and manipulation of generally less intrusive data. That is, computer surveillance and modern camera surveillance tend to work by gathering more information that is less invasive per datum, and then manipulating it through electronic methods to yield important information that normally would be obtainable only through more invasive surveillance techniques.

In some cases, such computer and high technology camera surveillance will be unable to yield serious benefits: Such surveillance should be discontinued for the simple reason that it is not effective. Where it is effective, and the public need great enough, the best way to achieve the benefits of surveillance while minimizing the threat to privacy is through use and disclosure limitations. Use and disclosure limitations will allow surveillance regimes to achieve the potential benefits of computer surveillance – the ability to reach conclusions from the collection and analysis of low-intrusive information that is akin to that traditionally achieved only through collection and analysis of high-intrusive information – while avoiding to the extent possible the privacy harms that accompany such surveillance.

The best way to achieve the benefits of computer surveillance while minimizing the privacy risks is to place greater focus on the later regulatory stages, and in particular, the final stage of public disclosure. If computer surveillance is likely to be effective, genuinely achieving a significant public good, widespread collection and analysis is necessary to achieve those benefits. The law should respond by adding new protections to the output end of the regulatory stage: The law should allow the collection and manipulation of data, but then place significant limits on the use and disclosure of the information.

Use Restrictions and the MONITOR Program

We can see how use restrictions can lead to best balance between security and privacy by returning to the MONITOR program of 2030. In that example, the public need was great. The threat was real. Plus, the system was designed to have the capacity to detect threats that could then be stopped. Some sort of monitoring program was necessary.

The mixed success of the MONITOR program was due to its mixed uses. MONITOR was used properly when it led to the capture of the South Loop Seven. This was the kind of use that its designers had in mind, and that most readers will applaud.

On the other hand, MONITOR was not created with clear limitations on its use. In particular, the example left open whether the information collected by MONITOR could be used to solve crimes. This presents a slippery slope. Once the information is created, there will be pressures to use it for a wider and wider range of government interests and a broader range of crimes.

Opinions will differ on where lines should be drawn. However, clear use

limitations could avoid the slippery slope altogether. A clear rule that MONITOR information could not be disclosed to criminal investigators under any circumstances could minimize the risk that MONITOR information could be used for less and less serious government interests.

The other uses of MONITOR were more obvious abuses. Employees misused the data for personal reasons instead of official ones. Data was disclosed inadvertently when an employee lost a laptop. Here the law should impose strict limitations on use and disclosure and ensure that they are enforceable. Data security is paramount, and remedies for violations should be harsh.

The broad lesson of MONITOR is that lawmakers should focus as much or more on the back end of surveillance systems as than the front end. If computerized surveillance systems can achieve critical public benefits that make them worthwhile, the emphasis should shift from whether the information can be collected to the legal limitations on how it is processed, used, and disclosed. The shift to computerization adds new steps, and the law must adjust to regulate them.

Courts or Congress?

The final question is what branch of government will create the use restrictions I have in mind. Can courts do this in the name of the Fourth Amendment? Or is it up to Congress?

In my view, it is up to Congress. The Fourth Amendment prohibits unreasonable searches and seizures. Use limitations are neither searches nor seizures, however. They are restrictions on what the government can do with information *after* it has searched for and seized it. As a result, there is little in the way of Fourth Amendment text, history,or precedent that supports recognizing use restrictions as part of Fourth Amendment protections.

Granted, it is possible to creatively re-imagine Fourth Amendment law in ways that recognize use restrictions. As far back as 1995, Harold Krent made such an argument.[1] Professor Krent reasoned that obtaining information is a seizure, and that the subsequent use of the information – including downstream disclosures of it – could make the seizure "unreasonable." In other words, instead of saying that searches and seizures occur at a specific time, they could be deemed to occur over a period of time. All uses of information would have to be reasonable, and courts could distinguish acceptable uses of information from unacceptable ones by saying that the former were reasonable and the latter were unreasonable.

The argument is creative, but I think it is too far a stretch from existing doctrine to expect courts to adopt it. In my view, there are two basic problems. First, most of the information collected by the Government is not protected under current Fourth Amendment law. Collecting third-party records is neither a search nor a

[1] Harold J. Krent, Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment, 74 Texas Law Review 49 (1995).

seizure (which is why it is frequently collected; information that is protected by the Fourth Amendment is collected only rarely). Under Professor Krent's proposal, however, presumably we would need to overhaul that doctrine to make all evidence collection a seizure to enable courts to then pass on the reasonableness of the seizure. If we took that step, however, we would need an entirely new doctrine on when seizures are reasonable, quite apart from downstream uses. This would require a fairly dramatic overhaul of existing Fourth Amendment law, all to enable use restrictions. (For a vision of such a dramatic overhaul, consider Christopher Slobogin's paper in this series.)

Second, disclosures of information come in so many shapes and sizes that courts would have little basis on which to distinguish reasonable from unreasonable uses. Every database is different, every data point is different, and every disclosure is different. The kind of fine-grained reasonableness inquiry called for by Fourth Amendment law would leave judges with few clear guide-posts to distinguish uses that violate the Fourth Amendment from those that don't with no historical precedent to follow. For both of these reasons, recognizing use restrictions in Fourth Amendment law may create more problems than it solves. At the very least, we should not expect courts to take such a leap any time soon.

In contrast, legislatures are well-equipped to enact use restrictions. They can promulgate bright-line rules concerning information collected under specific government powers, and they can explain the scope of the limitation and the contexts in which it is triggered. Further, they can legislate use restrictions at the same time they enact the statutes authorizing the evidence collection. That way, use restrictions can be a part of the original statutory design, rather than something imposed years later by the courts.

Governance Studies
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
www.brookings.edu/governance.aspx

Editors
Jeffrey Rosen
Benjamin Wittes

Production & Layout
John S Seo

E-mail your comments to gscomments@brookings.edu

Orin Kerr teaches criminal law, criminal procedure, and computer crime law at the George Washington Law School. His articles have appeared in the Harvard Law Review, Yale Law Journal, Stanford Law Review, Columbia Law Review, University of Chicago Law Review, Michigan Law Review, Virginia Law Review, New York University Law Review, Georgetown Law Journal, Northwestern University Law Review, Texas Law Review, and many other journals. According to the most recent Leiter Rankings, Professor Kerr ranks #7 among criminal law scholars in the United States for citations in academic journals. Kerr's scholarly articles also have been cited by most of the U.S. Courts of Appeals and over two dozen federal district courts.

Before joining the faculty in 2001, Professor Kerr was an honors program trial attorney in the Computer Crime and Intellectual Property Section of the Criminal Division at the U.S. Department of Justice as well as a special assistant U.S. attorney for the Eastern District of Virginia. He also is a former law clerk for Justice Anthony M. Kennedy of the United States Supreme Court and Judge Leonard I. Garth of the U.S. Court of Appeals for the Third Circuit. In the summer of 2009 and 2010, he served as special counsel for Supreme Court nominations to Senator John Cornyn on the Senate Judiciary Committee. In 2006, Kerr was a visiting professor at the University of Chicago Law School. In the Spring 2011 semester, he will be a visiting professor at the University of Pennsylvania Law School.

Professor Kerr is a co-author of the leading casebook in criminal procedure with Yale Kamisar, Wayne LaFave, Jerold Israel, and Nancy King, now in its 12th Edition. He is also a co-author of the leading treatise in criminal procedure (with LaFave, Israel, and King) and is the author of a law school casebook on computer crime law. Kerr is frequently interviewed by major media outlets, and his scholarship and advocacy have been profiled in the New York Times and National Public Radio.

The GW Law Class of 2009 voted to award Professor Kerr the Distinguished Faculty Service Award, the Law School's teaching award. Kerr has also represented criminal defendants in criminal cases. He recently briefed and argued a criminal appeal in the Sixth Circuit, and he represented Lori Drew pro bono against federal criminal charges brought in Los Angeles.

Before attending law school, Kerr earned undergraduate and graduate degrees in mechanical engineering. Kerr posts regularly at the popular blog "The Volokh Conspiracy," available at http://volokh.com. He is a member of the American Law Institute, and he was recently elected to the steering committee of the Criminal Law and Individual Rights Section of the District of Columbia Bar.