The Data Question: Should the Third-Party Records Doctrine Be Revisited?

POSTED AUG 01, 2012 09:20 AM CDT
BY ORIN KERR AND GREG NOJEIM

George Washington University law professor Orin Kerr and Greg Nojeim, senior counsel at the Center for Democracy & Technology, ponder how far the government can go in reading your email. Their essays can be found in Patriots Debate: Contemporary Issues in National Security Law, a book published by the ABA Standing Committee on Law and National Security and edited by Harvey Rishikof, Stewart Baker and Bernard Horowitz. The book can be ordered here (http://americanbar.org/groups/public_services/law_national_security.html).

INTRODUCTION

If a suspected thief has left written records of his crime in a friend's desk, can the police simply subpoena the friend for the records in the desk or should that be treated as a search of the suspect's property?

That question is at the heart of the "third-party records doctrine," which has provided guidelines for criminal investigations since the late 1970s. In essence, the doctrine holds that information lawfully held by many third parties is treated differently from information held by the suspect himself. It can be obtained by subpoenaing the third party, by securing the third party's consent or by any other means of legal discovery; the suspect has no role in the matter, and no search warrant is required.

Two well-known legal cases established the doctrine, United States v. Miller (1976) and Smith v. Maryland (1979). In Miller, the defendant attempted to suppress evidence that investigators had obtained from his bank, arguing that he had an expectation of privacy under the Fourth Amendment. The Supreme Court held that because checks and deposit slips sent to banks are freely circulated within the institution (the third party), Miller had no reasonable expectation of privacy, and that law enforcement did not need a search warrant to obtain the data.

In Smith, Michael Smith had robbed Patricia McDonough and then phoned repeatedly to threaten her. The police secured a pen register at the phone company (third party) to trace the numbers of calls placed to McDonough. Smith appealed his conviction, asserting that the pen register had violated his Fourth Amendment rights. Justice Harry A. Blackmun wrote that when Smith voluntarily "conveyed numerical information to the phone company and ... its equipment in the normal course of business, he assumed the risk that the company would reveal the information to the police."

As more and more information moves online, some have questioned whether this principle should continue to be applied. For example, in the Global Positioning System tracking case, U.S. v. Jones (2012), Justice Sonia Sotomayor's concurrence described the third-party records doctrine as "ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." The principle remains the same—suspects who entrusted their data to AT&T or Capital One in the 1970s are now entrusting their data to Google and Facebook. But the amount of data in the hands of third parties today is potentially much more revealing than in the 1970s. The question is whether that difference in quantity and quality has become a difference in kind.

GREG NOJEIM'S POSITION:
Why the Third-Party Records Doctrine Should Be Revisited

Under the third-party records doctrine, a person cannot assert a Fourth Amendment interest in information knowingly provided to a third party. If strict application of the doctrine ever served us well, it no longer does, leading to absurd results. This is particularly true in an age where so much more information is communicated through intermediaries. Proponents of the doctrine, quick to question what would limit it, fail to recognize that it already has holes that make its application uneven and illogical. It is time to turn the page and talk about limiting third-party records doctrine to preserve the role of the Fourth Amendment in protecting personal privacy.

The doctrine was forged at a time very different from our own. There was no email, and people communicated primarily by phone, fax and letter. There was no World Wide Web—if you wanted to find merchandise, you used the Yellow Pages. Cellular telephones were the stuff of science fiction. To put the period in perspective, the Vietnam War was winding down, Americans heard their music on eight-track tapes, and the Chevy Nova and Ford Maverick were the leading car models.

Today, we live much of our lives online. We make friends, receive news, execute purchases, conduct business, create documents, store photographs and find entertainment on the Internet. All of these interactions create records in the hands of third parties about our interests, problems, loves and losses, finances, associates, family moments, and even our location at any moment. In days past, law enforcement could obtain this information only with an enormous expenditure of resources. It had to tail suspects and query informants. Consequently, the public could have some confidence that when law enforcement officers sought such personal information, they would have strong evidence of a crime and focus their evidence collection on people likely tied to that crime. Fishing expeditions used to be expensive.

Today, the advance of technology has made it cheap and easy for law enforcement to gather this information secretly. The friction in the system and the practical anonymity that protected privacy are dissipating. And, with respect to law enforcement access, the third-party records doctrine has made it all possible.

The Supreme Court may not have been right when it decided U.S. v. Miller and Smith v. Maryland. Do people really “voluntarily” convey information to the phone company when they dial the numbers necessary to complete a call? And, if numbers dialed on a telephone are voluntarily conveyed to the phone company, isn’t the content of the call likewise voluntarily conveyed? Yet call content has been Fourth Amendment-protected since Katz v. United States in 1967.

The third-party records doctrine rests on a false notion of consent: A person who surrenders information to a third party consents to that third party’s disclosure of such information to others. In Fourth Amendment terms, their “expectation of privacy” is no longer “reasonable” because it is not reasonable to conclude that a third party will not disclose the information.

The reality is quite different, though, almost akin to compelled consent, which is not consent at all. If you want to communicate efficiently today, your communications likely will go through your ISP’s servers. The alternative means of communication either involve conveying information to other third parties, or traveling to the other communicant so you can have a personal chat. Consent in this context has little meaning.

For too long, application of the third-party records doctrine has permitted absurd results. A person who stores documents and items in a physical space controlled by a third party in the business of renting it out retains a Fourth Amendment interest in those items. But if she stores the same information with an online lockbox in the business of providing on-line document storage services, she loses that Fourth Amendment protection and it is available to law enforcement with a mere subpoena.
Some worry that without the third-party records doctrine, clever criminals would convey evidence of their crimes to third parties so that it would enjoy constitutional protection it otherwise would lack. Criminals would substitute third-party services for activities that would otherwise be conducted in the open. But this proves too much: Innocent people would overwhelmingly constitute the group of “substitutors.” The third-party records doctrine dissuades them from using the most desirable paths of communication by diminishing the privacy that would otherwise attend to them. For example, if the most efficient way for a group to edit a sensitive document is to store and edit it “in the cloud,” why drive the group toward less efficient solutions that don’t involve an intermediary? That’s what the third-party records doctrine does.

Some argue that the third-party records doctrine is simple for the courts to apply, and abandoning it or carving out exclusions would leave the courts at sea. They struggle to apply the “reasonable expectation of privacy” test and reach contradictory results when they do. Moreover, perhaps ease of application of a rule ought not to be the determinative factor in setting such a rule when a fundamental right is at stake.

Where the third-party records doctrine would lead to undesirable results, Congress has sometimes stepped in with legislation to extend privacy protections to particular categories of data. For example, the Right to Financial Privacy Act protects financial records, the Video Privacy Protection Act protects video rental records, and the Health Insurance Portability and Accountability Act protects medical records. However, each of these privacy statutes comes up short. They fail to extend the same protection that would come with full extension of Fourth Amendment protection to the records in question.

For example, the Electronic Communications Privacy Act requires a warrant based on a showing of probable cause for law enforcement access to the contents of electronic communications only for the first 180 days of the life of the communication. If a person’s provider of electronic communications service holds the communications content for a lengthier period, the warrant requirement expires and law enforcement accesses the records with a mere subpoena. The government, exploiting inartful language in the statute, takes the position that it can obtain opened email from a provider without getting a warrant no matter the age of the email, leading to the absurd result that the spam email you never open is better protected than the personal email you do. Worse still, the ECPA provides that the information you outsource for storage and computing purposes is not subject to the warrant requirement at all, no matter its age and even though it is content.

The protections afforded by the ECPA are no substitute for the warrant requirement that would attend full extension of Fourth Amendment protections to communications content in the hands of third parties. Like the ECPA, the other privacy statutes that protect some categories of sensitive personal information generally do not require warrants for law enforcement access.

Professor Kerr agrees in a blog post for the Volokh Conspiracy that full Fourth Amendment protection should be afforded communications content, and he applauded when the 6th U.S. Circuit Court of Appeals at Cincinnati reached that conclusion in U.S. v. Warshak (2010). The court reasoned that email today is analogous to a letter or a phone call, the contents of which are protected by the Fourth Amendment.
though each is conveyed through a third-party post office or telephone company. So there is consensus between us that at least one category of information—communications content—retains Fourth Amendment protection though conveyed through a third party. This is a chink in the armor of the third-party records doctrine.

Why, though, stop there? Is there no information, or collection of information, other than content that warrants Fourth Amendment protection when held by a third party? The *Smith* court may have thought so. It based its decision in part on the fact that numbers dialed on a telephone and conveyed to the phone company to complete a call revealed little information—not the purpose of the communication, not the identity of the parties communicating, and not even whether the call was completed. This invites one to consider whether much more revealing noncontent information would retain Fourth Amendment protection even if conveyed to a third party. While there might be a period of uncertainty while courts fill in the contours of the noncontent information protected, that is no different from the way the courts have provided clarity to the application of other rights.

The Supreme Court’s January decision in *U.S. v. Jones* may have shed some light. *Jones* did not involve third-party records—law enforcement agents tracked the defendant directly for 28 days by secretly attaching a GPS device to the vehicle he drove. The court held that attaching a GPS device to collect location information was a Fourth Amendment search. While attaching the device was a “trespass” central to the court’s ruling, five justices signed concurring opinions that suggest that precise, pervasive monitoring of one’s location could trigger Fourth Amendment protection without a trespass. This could bolster arguments that cell site location information generated by use of a cellular telephone is sufficiently sensitive to warrant Fourth Amendment protection though obtained from a third-party service provider. Two federal district courts, in the Eastern District of New York and the Southern District of Texas, have already reached that conclusion.

Accumulations of location information held by cellular telephone service providers might be one category of records to which Fourth Amendment protection should attach. What principles would limit the third-party records doctrine and determine the types of information that should retain Fourth Amendment protection though held by a third party? Scholars are already considering that question. Some say that one factor should be the relative sensitivity of the information, as the court already hinted in *Smith*. Another might be whether the information is in fact knowingly “volunteered” to the third party. Still another might be whether the third-party record holder has a relationship akin to a fiduciary relationship with the party to whom the record pertains.

The courts will ultimately determine the factors limiting the third-party records doctrine so that Fourth Amendment protection extends to information other than content. So that the Fourth Amendment retains its vitality in a networked society, it is important that they start right away.

**ORIN KERR’S COUNTERPROPOSAL:**

**The Case for the Third-Party Doctrine**

I’m delighted to debate Greg Nojeim on the controversial third-party doctrine of Fourth Amendment law. Greg and I share a number of first principles: Both of us are looking for a way to apply the Fourth Amendment to new technologies in a sensible and balanced way. Our disagreement is on how to do that. Greg would reject the third-party doctrine, while I would apply the doctrine in some cases but not in other cases. In this contribution, I want to explain why I think that the much-maligned third-party doctrine is a critical tool for applying the Fourth Amendment to new technologies in some cases, but that it should not be extended to all cases.

My argument rests on the need to maintain the technological neutrality of Fourth Amendment protections. The use of third parties is akin to new technology, and that technology threatens to alter the balance of power struck by the Fourth Amendment. The third-party doctrine offers a way to maintain the balance of police power: It ensures that the same basic level of constitutional protection applies regardless of technology. Or so I will argue, drawing from two recent articles of mine: “The Case for the Third-Party Doctrine” and “Applying the Fourth Amendment to the Internet: A General Approach.”

My argument begins with a thought experiment. Let’s start by imagining a world without third parties. If you want to send a package to a friend, you need to leave your home and carry it to your friend’s house. If you want to go to the doctor’s office, you need to visit it in person. In a world without third parties, you would need to venture out into the world on a regular basis to accomplish anything.

Next, ask yourself how the Fourth Amendment would apply to police investigations in this world with no third
parties. The rules would be simple. The police would need a warrant to enter your home, but they would be permitted to watch you in public. They could watch you leave your home, travel to the home of your friend, and disappear inside when you delivered your package. They could watch you leave your home, go to the doctor’s office and disappear inside. All of these steps would occur in public, where the Fourth Amendment offers no protection from the watchful eye of the police.

Now let’s introduce third parties. Third parties allow individuals to do remotely what they would otherwise have to do in person. Instead of traveling to your friend to deliver the package, you can send the package through the postal mail. The postal network substitutes for your trip to your friend: Instead of bringing your package to your friend, the mailman will do it. And instead of visiting the doctor in person, you could call the doctor on the phone. To borrow from the old advertising campaign for the Yellow Pages, you can “let your fingers do the walking.” In each case, the third-party service means you no longer have to leave your home.

The critical point from the standpoint of Fourth Amendment law is that use of third parties introduces a substitution effect. In a world with no third parties, individuals often have to travel in public. The police can see when individuals leave their homes, where they travel and when they arrive. Using third parties allows individuals to substitute a private transaction for that public transaction. Facts that used to be known from public surveillance are no longer so visible. By allowing individuals to use remote services, the use of third parties has brought outdoor activity indoors.

The question for Fourth Amendment law is how to respond to this technological shift. In my view, the goal should be to apply the Fourth Amendment in a technologically neutral way. In a world with no third parties, the Fourth Amendment strikes a balance of police power: It gives the government the power to investigate crimes in some ways, but also limits the government’s investigations in important ways. I think that’s a sensible balance, as it tries to balance our shared interests in deterring crime and punishing wrongdoing (which can only occur if the police successfully gather evidence to prove cases) with our commitments to privacy and avoiding government abuses of power. If I’m right that this balance is proper, then it follows that we should maintain it: We should try to apply the Fourth Amendment so that it offers the same basic protections and strikes the same balance in a world of third parties as it did in a hypothetical world without them.

The third-party doctrine achieves that, in my view. The doctrine ensures that the Fourth Amendment applies to conduct that harnesses third parties in the same way it applies to events that occur without third-party help. It does so by matching the Fourth Amendment protection in the use of the third party with the Fourth Amendment protection that existed before.

Smith v. Maryland is a good example. In Smith, a robbery victim was receiving harassing phone calls. The police suspected Smith, and they asked the phone company to install a pen register on his home phone line. Whenever a call was placed from Smith’s home phone, the phone company would record the numbers dialed and keep a record for the police. The record showed that the calls did indeed originate from Smith’s home, and the police used that evidence to get a warrant to search the home and prove Smith’s guilt. The question in the case was whether the numbers dialed were protected by the Fourth Amendment.

The court in Smith ruled that Smith had no reasonable expectation of privacy in his numbers dialed. That rule maintained the level of Fourth Amendment protection regardless of whether Smith used a third party to harass his victim. By holding that the use of the pen register did not constitute a search, the court ensured that the police would have the same information either way. The time of the call, the originating number of the call, and the destination of the call are the informational equivalents of what the police would have learned by watching Smith in public if he had not used a third party. In other words, Smith could not change the balance of Fourth Amendment protection by using a third party: The Fourth Amendment offered the same level of protection either way.

Importantly, my defense of the third-party doctrine implies an important limit: The doctrine should apply when the third party is a recipient of information, but it should not apply when the third party is merely a conduit for information intended for someone else. Put another way, the third-party doctrine should apply to the collection of
noncontent information in a network but not the contents of communications. The reason is that when the third party is merely a conduit for information, the information that is sent through the third party is not information that would have been revealed if no third parties had been used. In a world with no third parties, the message would remain private: if I bring you a sealed package in person, the government can’t open up the package without a warrant. That same rule should and does apply if the delivered communication takes the form of a sealed letter in the postal mail, the contents of a phone call, or the contents of an email.

Nojeim makes several rejoinders to my approach. First, he argues that use of third parties is unavoidable in our modern world. That may be right, but the same was true about going out in public in the world without third parties. It would be unpersuasive to argue that the Fourth Amendment must protect what occurs in the public square because venturing out into the public square is unavoidable in our modern life. In my view, it is equally unpersuasive to claim that the Fourth Amendment must protect third-party substitutes because modern life requires their use.

Second, Nojeim argues that surveillance is cheaper and easier today than it used to be, and therefore that there is more of a need for legal regulation. Cost and time used to limit the government and channel its resources into the more important investigations and away from abuses; if the costs and time of surveillance drop, more abuses are likely unless the law steps up its role. This may be right. But Nojeim does not say why we should rely on the courts, rather than Congress, for this source of law. In my view, statutes are ideally situated to provide the kind of counterweight Nojeim envisions. Statutes have the flexibility to offer a tailored and nuanced approach to limit government properly without the blunt instrument of the Fourth Amendment and the warrant requirement.

Third, Nojeim suggests that it is arbitrary to apply the third-party doctrine to noncontent information but then reject its application to the collection of contents. In his view, limiting the third-party doctrine to noncontent information is “a chink in the armor” of the doctrine. But legal doctrines should apply to the extent of their rationale, and no further. Recognizing the validity of the third-party doctrine in some cases does not mean that it should logically apply to cases that are very different. In my view, countering the substitution effect of using third parties generates a sensible and reasonably clear rationale for both the presence of the third-party doctrine and its limits. To ensure the technological neutrality of the Fourth Amendment, we should apply the third-party doctrine where third parties generate substitution effects but not where they don’t. This means that courts should apply the third-party doctrine to the collection of noncontent information, but should reject the doctrine when the government collects contents of communications.

GREG NOJEIM’S REBUTTAL:

As Orin Kerr points out, we do have some points of agreement. We both agree that the third-party doctrine should not apply to content held by third parties: A warrant should be required for content. Professor Kerr would stop there; I would not. I would not reject the third-party doctrine, but instead I urge more exceptions to its application. Content is not the only piece of information that should enjoy Fourth Amendment protection though held by a third party.

Professor Kerr does not contest my point that the court’s explanation for adopting the third-party doctrine in Smith v. Maryland rests on shaky ground. It reasoned that consumers voluntarily convey to the phone company the numbers they dial when placing a call, that they therefore have no reasonable expectation of privacy in that information and have consented to further disclosure of this information to law enforcement. Perhaps we agree as well that “consent” in some scenarios in which the third-party doctrine applies is not really voluntary.

We also both agree that the Fourth Amendment should be applied to new technologies in a way that preserves the balance between privacy and law enforcement interests. I believe that the third-party doctrine has thrown that balance off. Technology permits us to communicate privately with people who are distant and numerous, but third parties often convey those communications. When they do, Fourth Amendment protections are lost.

Professor Kerr argues that requiring communicants to meet in person so law enforcement can observe them (but not listen in) maintains the balance by precluding a substitution effect. He worries that without the third-party doctrine obliterating constitutional protection that might be afforded information about communications—the parties who communicated, the time of the communication, the length of the communication, the frequency with which they communicated, the location of the communicants and the means by which the communication occurred, etc.—the bad guys would gain Fourth Amendment protection by using third parties instead of showing
This is not so. First, most communicants simply cannot meet in order to exchange information. It is not practical to do so, particularly where the communicants are far apart or are numerous, as occurs much more frequently today than in the past. There is no substitution effect to worry about because there is no practical alternative to use of the third party to convey the information. The alternative is not to show up personally so the police can watch; rather, as a practical matter, the alternative when one wants to have a Fourth Amendment-protected communication is not to communicate at all.

Second, to the extent that there is a substitution effect, it falls primarily on people who are not involved in criminal activity because the overwhelming majority of communicants are not criminals. We should be more worried about people substituting less efficient means of communicating—showing up in person—in order to protect the privacy of information about their communications.

Instead of advancing technological neutrality, the third-party doctrine threatens it. The law is technologically neutral if the level of protection that information enjoys does not change when different platforms are used to convey the information. When the platform involves a third party, Fourth Amendment protection is often lost; but when the platform does not involve a third party, Fourth Amendment protection remains.

We agree that Congress ought to step in with statutory protections when application of the third-party doctrine leaves sensitive information unprotected from law enforcement access. But Congress generally legislates a weaker protection regime than the Fourth Amendment would require. For instance, Congress passed a law that is contrary to the rule about which we both agree: That the warrant requirement should apply to content held by third parties. Instead of requiring a warrant, the ECPA allows law enforcement to use a subpoena when it seeks the contents of a document you have stored with a third party, the contents of your sent email, and the contents of any message sent to you more than 180 days ago. There is no judicial authorization and no determination of probable cause, and notice that law enforcement has accessed this information is often delayed.

We both agree this should be changed. We may agree that other privacy statutes should also be strengthened. But I believe that court-authorized expansion of the list of exceptions to the third-party doctrine should also be part of the solution.

ORIN KERR’S CLOSING:

Greg Nojeim and I have a relatively narrow disagreement: When applying the Fourth Amendment to a network, how far should the third-party doctrine extend to ensure that Fourth Amendment rules remain technologically neutral?

In my view, the third-party doctrine should not apply to contents of communications sent over networks but should apply to noncontent information. Nojeim agrees with me that the third-party doctrine should not apply to contents. But he parts ways with me and argues that the third-party doctrine should apply to at least some noncontent information. Nojeim does not specify which noncontent information should fall within the doctrine, but he advocates a “court-authorized expansion of the list of exceptions to the third-party doctrine” to cover at least some noncontent information.

Our disagreement appears to hinge on a critical assumption. When we make the comparison across technologies, what starting point should be used? How much privacy do we enjoy on the baseline of a world without third parties, so that we can make a proper comparison to determine if a legal rule operates in a technologically neutral way?

In my view, history and tradition provide the proper baseline. Historically, when two people wished to communicate, they needed to do so in person. They needed to travel out in the open to meet somewhere. An observer wishing to watch them would be able to track their public movements. The observer would know when they walked to the meeting place, when they arrived and when they left. To be sure, the outside observer would not know what the two people said to each other: The actual contents of the communication would be hidden from observation. But the information about the communication—who went where, and at what time, and for how long—could be observed in public.

Applying the third-party doctrine to noncontent information but withholding it from content information re-creates this basic division for a networked world. It maintains the prior level of government power by ensuring that the contents of the communications remain protected and yet the noncontent information about the
communication—who went where, and at what time, and for how long—can still be observed. And it maintains that balance regardless of the particular network in question: The same balance applies if the network is the postal network, the telephone network or today’s Internet.

When the third-party doctrine is appropriately limited to noncontent information, the doctrine does not cause the imbalance that Nojeim suggests. The scope of privacy over communications networks remains the same as the scope of privacy in the physical world. It extends Fourth Amendment protection in some contexts and withholds it in other contexts, just as does the Fourth Amendment when applied to physical space.

A former special assistant U.S. attorney for the Eastern District of Virginia, Orin Kerr served as a law clerk to U.S. Supreme Court Justice Anthony M. Kennedy and was special counsel for Supreme Court nominations to U.S. Sen. John Cornyn, R-Texas.

Greg Nojeim previously was counsel with the American Civil Liberties Union and at the American-Arab Anti-Discrimination Committee. He also worked at the D.C. office of K&L Gates. He is a former co-chair of the Coordinating Committee on National Security and Civil Liberties of the ABA Section on Individual Rights and Responsibilities, a perch from which he helped draft the ABA’s 2007 policy on the state secrets privilege.