StingRay Technology and Reasonable Expectations of Privacy in the Internet of Everything

*By Howard W. Cox**

Note from the Editor:

This article discusses cell site simulators, also known as StingRays, and the 4th Amendment issues they raise in light of changing technology. The Federalist Society takes no positions on particular legal and public policy matters. Any expressions of opinion are those of the author. Whenever we publish an article that advocates for a particular position, as here, we offer links to other perspectives on the issue, including ones opposed to the position taken in the article. We also invite responses from our readers. To join the debate, please email us at info@fedsoc.org.

• *StingRay Tracking Devices*, ACLU, *available at* https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices.

• *Cell-Site Simulators*, Electronic Frontier Foundation, *available at* https://www.eff.org/sls/tech/cell-site-simulators.

• Joseph Lorenzo Hall, *Previewing Tomorrow's Location Privacy Hearing: GPS vs. Cell Tower Tracking*, Center for Democracy & Technology (April 24, 2013), *available at* https://cdt.org/blog/previewing-tomorrows-location-privacy-hearing-gps-vs-cell-tower-tracking/.

• Stephanie Pell & Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap*, 16 Yale J.L. & Tech. 134 (2014), *available at* http://yjolt.org/lot-more-pen-register-and-less-wiretap.

As Americans become more attached to their electronic devices, they expect them to be available at all times and places, and to connect with each other seamlessly and continuously through the "Internet of Everything." Law enforcement is developing tools to take advantage of the technology enabling this omnipresent connectivity. Those tools, designed to find criminals and the devices they carry, present unique challenges in applying traditional Fourth Amendment concepts of reasonable expectations of privacy to twenty-first century electronic communications.

The case of *Jones v. U.S.*, currently on appeal before the District of Columbia Court of Appeals, provides an appropriate context for the high technology struggle between the privacy bar and the needs of law enforcement.[1] In 2014, Prince Jones was convicted of robbing three women and raping two of them. During the 2013 attacks, he also stole the cell phone of one victim. Guessing he would use the stolen phone, DC police used a portable cell-site simulator to track down the location of the phone. DC police believed there were exigent circumstances present (they assumed he would use the cell phone for a limited period of time then quickly discard it), and therefore did not obtain a warrant to use the cell-site simulator. The cell-site simulator led DC police to a car in a parking lot, where they found and arrested Jones. His appeal directly challenges the warrantless use of cell-site simulator technology.[2]

This article will examine current issues regarding the government's use of cell-site simulators, commonly known as "StingRay" devices, to identify and track cell phones used in criminal activity. It will also examine the confusion faced by courts in applying traditional privacy principles to "self-connecting devices" such as cell phones, which automatically broadcast identification data with little or no user interface. Courts have not demonstrated an appropriate understanding of legitimate user expectations of privacy in self-connecting cell phone technology, specifically with respect to StingRays capturing information broadcast by this technology. This lack of understanding is, in part, the result of an unprecedented level of secrecy that the FBI has insisted upon regarding the use of this technology. This secrecy has been exploited by members of the privacy bar attempting to establish unreasonable standards for the expectation of privacy in self-connecting cell phone communications. The article concludes that, given the level of connectivity that is inherent in the use of modern smartphones, it is virtually impossible to establish a Fourth Amendment reasonable expectation of privacy in connectivity data, and that Congress is in the best position to establish statutory limits in this area.

I. What is a StingRay Device?

A StingRay is a device used by law enforcement to identify information broadcasted by a cell phone during its normal operation.[3] By the inherent design of cell phone technology, all cell phones constantly "self-connect" with cellular carriers via cell towers. This feature allows the device to identify and connect with the tower with the best local signal, and maintain the strongest possible signal. The presence and status of this

** Howard W. Cox is a former federal prosecutor and Senior Intelligence Service officer. After almost 40 years of federal service, he retired as the Assistant Inspector General for Investigations of the Central Intelligence Agency. Prior to his employment with the CIA, Mr. Cox was the Assistant Deputy Chief of the Computer Crime and Intellectual Property Section of the Department of Justice, where he was responsible for supervising criminal prosecutions of federal hacking and identity theft cases. While at the Department of Justice, Mr. Cox received the Attorney General's Distinguished Service Award. Mr. Cox is currently an adjunct professor at George Washington University, where he teaches graduate level courses in computer forensics. He received his AB degree from Seton Hall University, South Orange, NJ, and his law degree from Georgetown University Law Center, Washington, DC.*

ongoing communication is displayed on the phone (the number of "bars" showing the strength of the signal). To establish and maintain connectivity, cell phone devices constantly provide cell towers and cell service providers with a variety of information, some of which is unique to a particular device.[4] Furthermore, if a telephone call is made or received by the device, the device will provide additional information to the cell tower and service provider, including the phone number registered to the device, the number of the call dialed or received, and the date, time, and duration of the call.[5] StingRays can mimic cell towers, and law enforcement employs them in ways that are designed to provide the target device with the strongest local cellular signal, thereby causing the device (and any other active cell phones within range) to establish connectivity with the law enforcement provided cell-site. Once this connectivity is established, the device provides the law enforcement cell-site with the connectivity data, known as cell-site location information (CSLI), which is normally provided to the local cell tower and ultimately to the cell service provider.

It is important to note that, when operated in this manner, the StingRay device does not capture the content of communications. As will be discussed below, law enforcement requests to the courts to use StingRays are based upon the authorities set forth in the Pen/Trap Statute[6] and the Stored Communications Act (SCA)[7] regarding court orders for non-content "electronic communications,"[8] and Rule 41 of the Federal Rules of Criminal Procedure regarding search warrants. These requests have all sought connectivity data, not the content of communications (i.e. the words exchanged in a conversation held using the device). Interception of content in real time would indisputably require a wiretap order under Title III, but the issues surrounding collection of CSLI are more complicated.[9]

The growth in the general use of cell phones is mirrored by the growth in their use in the commission of crimes. StingRays have proven to be vital in assisting law enforcement in identifying the presence and use of cell phones used in crimes. They are particularly important when law enforcement is seeking to identify the presence of "burner" phones. These inexpensive devices are used once or for a limited time, and then disposed of and replaced by new burner phones. They are often bought by criminals using stolen identity or credit card information. StingRays devices can also be used by law enforcement to identify the location of "air cards."[10]

Growing law enforcement use of StingRay technology reflects the growth of cell phone use. It has been reported that numerous federal law enforcement agencies in DOJ, the Department of Homeland Security (DHS), and the Department of the Treasury are currently using some form of StingRay technology.[11] It has also been reported that over 60 state and local law enforcement agencies have used StingRay technology in hundreds of cases.[12] StingRays can be mounted in vehicles and aircraft or used as hand held devices.[13] This growth has fueled increasing alarm in the privacy bar regarding the law enforcement use of the technology, and the perceived lack of appropriate legal authority by which it is justified. For example, the American Civil Liberties Union (ACLU) has criticized both the use of the technology and the secrecy that surrounds its use.[14] One chapter of the ACLU has even prepared a primer for defense counsel on how to challenge the use of StingRay technology.[15]

II. Challenges to Law Enforcement Use of StingRay Technology

A. Legal Standard for Application

Traditionally, prosecutors have sought court authorization to deploy StingRay devices to locate telephones in criminal investigations.[16] The traditional approach has been to seek a court order under the Pen/Trap Statute.[17] This statute allows prosecutors to apply, *ex parte*, for an order authorizing the government to deploy a device that captures non-content information. Unlike search warrants or Title III wiretap orders, the Pen/Trap Statute merely requires that the government establish that the information likely to be obtained is relevant to an ongoing criminal investigation.[18] (Some courts have ruled that this is the equivalent of the "reasonable suspicion" standard).[19] The Pen/Trap Statute was passed following the holding of the Supreme Court in *Smith v. Maryland*, which held that telephone users have no reasonable expectation of privacy in the phone numbers which they dial.[20] In light of the Court's holding that there were no Fourth Amendment restrictions on warrantless government access to this data, Congress created procedural protections designed to establish standards and accountability in the government's use of this technology.[21] At times, prosecutors have also sought a "hybrid" order, seeking authority under the Pen/Trap Statute and the SCA.[22] The hybrid order is intended to address possible limitations of the scope of the Pen/Trap Statute, as it applies to the capabilities of the StingRay device.[23]

The privacy bar and some academics have insisted that, at a minimum, applications for deployment of StingRay devices should be based on search warrants issued upon findings of probable cause.[24] Federal court reactions to this challenge has been mixed. While there are no federal appellate decisions regarding StingRay applications,[25] and relatively few lower federal court rulings,[26] litigation regarding StingRay is related to a larger fight over the legal standard to be used when the government seeks to obtain historic and prospective CSLI from carriers.[27] Once again, the government has historically relied upon the the court order authority of the Pen/Trap Statute and the SCA to obtain CSLI data from cell phone carriers.

In a number of recent decisions, federal appellate courts have provided unusually mixed signals on the legal standard needed to obtain CSLI from carriers. In a Solomonic decision, the Third Circuit ruled that the Pen/Trap Statute's "reasonably related to a criminal investigation" standard was appropriate, but that issuing magistrates were free to impose a higher probable cause search warrant standard.[28] In *U.S. v. Graham*, a divided panel of the Fourth Circuit ruled that cell phone customers had a reasonable expectation of privacy in CSLI data provided to their carriers, and that a search warrant would be required to obtain it.[29] While the panel's decision could have provided some certainty on the search warrant requirement, the holding's precedential value is now in doubt because the Fourth Circuit recently agreed to rehear the matter *en banc*.[30] The Fifth Circuit has ruled that the SCA provides sufficient authority to obtain historic CSLI without a warrant.[31] In *U.S. v. Skinner*, the Sixth Circuit clearly ruled that cell phone customers had

no reasonable expectation of privacy in information that they voluntarily provided to their service providers, and that a search warrant was not required.[32] Lastly, the Eleventh Circuit recently reversed its position in *U.S. v. Davis*. As originally decided, a unanimous panel of the court ruled that customers had a reasonable expectation of privacy in historic CSLI provided to their carriers, and that a search warrant would be required to obtain this data.[33] However, upon *en banc* review, the full court rejected the panel's reasoning and concluded that the authority of a court order under the SCA was sufficient to obtain historic CSLI without a warrant.[34]

In many of the reported decisions regarding StingRay applications, the government initiated the application process by conceding the need for a search warrant, or by arguing that the court's order under the Pen/Trap Statute or SCA should be based on a probable cause standard. For example, in *In the Matter of an Application of the U.S. for an Order Relating to Telephones Used by Suppressed*, the magistrate judge imposed extensive controls on the government's use of StingRay technology.[35] What the court's opinion does not really highlight is the fact that, from the outset of the case, the government was applying for a warrant.[36] Similarly, in *U.S. v. Rigmaiden*, the government's application was based on a DOJ concession that a warrant would be required.[37]

Despite the fact that a clear majority of appellate courts have approved the government obtaining historic and prospective CSLI data without a warrant in cases not dealing with StingRay, DOJ has been reticent to use the lesser standard in its applications for StingRay devices. In recent practice and official policy, DOJ has instead chosen to seek StingRay authority under a search warrant standard. Its reticence may be a capitulation by DOJ to the privacy bar, or it may be a response to real or perceived pressure from Congress. Congress has created statutory rights of privacy and procedure following the Supreme Court's past determinations that such rights were not constitutionally required. When the Supreme Court ruled in *Smith v. Maryland* that persons had no reasonable expectation of privacy in dialed phone numbers,[38] Congress passed the Electronic Communications Privacy Act (ECPA)[39] and the Pen/Trap Statute to create non-constitutional statutory controls on the government's access to this data. When the Court ruled in *U.S. v. Miller*[40] that notice and an opportunity for a hearing were not constitutionally required when the government sought records in the hands of third parties, Congress created procedural requirements through the Right to Financial Privacy Act.[41]

B. The New DOJ Policy

Influential House and Senate members have also sought to pressure DOJ to adopt a policy of obtaining warrants when applying for StingRay authority. In 2014, following private meetings between DOJ representatives and staffers of Senators Charles Grassley and Patrick Leahy of the Senate Judiciary Committee, the FBI instituted an internal policy that most FBI StingRay applications would be based upon a search warrant standard.[42] More recently, in response to similar pressure from the House Committee on Oversight and Government Reform, DOJ announced a policy seeking to submit most federal law enforcement StingRay applications to a warrant standard.[43]

The recently issued *DOJ Policy Guidance* document commits DOJ prosecutors to basing their applications for cell site simulators on warrants issued under Rule 41 of the Federal Rules of Criminal Procedure (unless the applications are based on certain exigent and exceptional circumstances). The document also sets forth other controls regarding senior official approval, record keeping, and training.[44]

Typically, policy statements like this do not apply to the operation of non-DOJ law enforcement agencies unless some other law or policy commits those agencies to follow the DOJ policy.[45] However, the cell-site simulator policy has a number of controls that ensure its uniform use throughout federal law enforcement. For example, the policy states that all federal applications for StingRay technology must comply with the policy. Since all federal agents must apply for warrants or orders through a federal prosecutor, the DOJ policy will ensure uniform application of the policy. Furthermore, in response to pressure from the same House and Senate committees, many federal law enforcement agencies outside of the DOJ have made separate commitments that mirror the DOJ policy guidance.[46]

On the state and local levels, at least twelve states have passed laws mandating that law enforcement use of a cell-site simulator must be based upon a court issued search warrant based upon a finding of probable cause.[47]

C. Secrecy Surrounding the Use of StingRay Devices

Despite the legislative scrutiny, federal use of StingRay devices has been shrouded in secrecy. While law enforcement has a right to and often does protect sources and methods, the FBI has imposed unusual controls over the extent to which StingRay technology can be described in applications for court orders or warrants, and in subsequent criminal proceedings. This secrecy has been noted by the privacy bar in support of its portrayal of StingRay as some sort of spy or military technology deserving special scrutiny by the courts. Privacy advocates have also alleged that the government has not been candid with the courts when describing the capabilities of the technology and its use by the government.[48] While most of these charges are without merit, the unusual level of secrecy has understandably increased judicial, legislative, and public scrutiny.

The FBI has, in numerous cases, forbidden local law enforcement agencies to purchase and use StingRay and related technology unless they agree to significant restrictions on publicly releasing information about it. The extent to which the FBI and Harris Corporation, the manufacturer of StingRay, have sought to restrict the discussion regarding the capability and use of the StingRay device is set forth in a remarkable nondisclosure agreement (NDA). [49] The NDA appears in a letter from the FBI to Baltimore police and prosecutors. In the letter, the Acting Director of the FBI's Operational Technology Division cites the need to protect sensitive law enforcement sources and methods, and insists that Baltimore officials agree not to mention the device, its capabilities, or any literature relating to it in any court proceeding (including warrant applications, grand jury proceedings, pre-trial discovery, trial, or appeal) without prior notice to the FBI. Baltimore officials also agreed that if the FBI determined that the use or description of the technology in a court proceeding would potentially or actually compro-

mise the technology, the FBI could request that the charges be dismissed; upon such a request, the Baltimore officials agreed to seek dismissal of the underlying charges.[50] While it is not unheard of for prosecutors to dismiss charges to protect sources and methods, this level of non-disclosure regarding StingRay devices is unusually high. Some commentators have speculated that, in addition to the dismissal of state charges, federal charges in certain cases have also been reduced or dismissed by federal prosecutors, to avoid disclosure regarding the use and capabilities of StingRay technology.[51]

Of particular concern to certain courts and legislators is the possibility that prosecutors are less than candid in warrant applications regarding the anticipated uses of StingRays. As a result, some courts have gone to extraordinary lengths in placing restrictions on the use of StingRay technology. In one recent decision, the issuing magistrate expressed frustration with how little information was provided by the government, stating that he was forced to do independent research on the capabilities of the StingRay device because he suspected that the conditions of an NDA precluded the federal prosecutor and case agent from being appropriately responsive to his questions.[52]

Some have suggested that the terms of the NDAs have prevented federal prosecutors from fully developing the record regarding the actual uses of StingRay devices, and demonstrating to courts that the devices are being used appropriately, within the requirements of existing law. For example, members of the privacy bar have stressed that StingRay devices are capable of capturing the content of communications, the warrantless collection of which violates Title III. They also allege that because these devices establish connectivity with all local cell phones, that such connectivity results in an "overcollection" of information on innocent parties. These arguments reflect a lack of understanding of how StingRays are deployed, and how traditional controls over law enforcement surveillance technology are applied to StingRay usage.

Under traditional trap and trace orders for telephone information obtained under the Pen/Trap Statute, law enforcement has often used a device known as a Dialed Number Recorder (DNR). While these devices capture dialing information authorized by the Pen/Trap Statute, they also have the *capability* to intercept content of communications, which is beyond the scope of the Pen/Trap Statute. Law enforcement agencies routinely put procedures in place to ensure that this additional capability is not enabled when the DNR is used to capture Pen/Trap data.[53] In addition to these internal procedures, the Pen/Trap Statute has always included direct limitations on using Pen/Trap authority to capture contents of communications.[54] The statute also sets forth significant controls regarding record keeping about the use of this technology.[55]

Privacy bar concerns related to the overcollection of innocent third party connectivity data beyond that of the target phone fail to recognize that DOJ, the courts and Congress have recognized that the possibility of overcollection is inherent in the deployment of many kinds of law enforcement surveillance technology. Legitimate concerns have been addressed through a variety of technological and procedural controls to minimize overcollection. For example, in 2002, DOJ issued a policy document entitled "Avoiding Collection and Investigative Use of 'Content' in the Operation of Pen Registers and Trap and Trace Devices."[56] Furthermore, in its September 2015 policy statement on cell-site simulators, DOJ specifically defined and applied overcollection controls to data gathered by cell-site simulator devices.[57]

However, overcollection of cell phone data remains an issue of judicial concern. For example, law enforcement will try to determine if a subject was in range of particular cell phone towers by requesting from a cellular service provider a "dump" of all historic data regarding particular towers during a period of time.[58] This dump enables the government to search the data for evidence of the target device or person within the range of cell tower. The privacy bar has contended that the production of information on non-target devices is beyond the authority of the SCA.[59] To date, most courts have agreed that the SCA authorizes the production of this historic data from cell carriers without a warrant, including information about non-target phones.[60] However, at least one court has cautioned that a different outcome might be compelled when prospective data is sought via a cell-site simulator.[61]

III. Is There a Reasonable Expectation of Privacy in Self-Connecting Devices?

Traditional Fourth Amendment jurisprudence holds that the government is usually required to obtain a warrant when conducting a search in an area where a person has a reasonable expectation of privacy. The reasonable expectation of privacy analysis, driven by Justice Harlan's concurrence in *Katz v. U.S.*,[62] is based on two factors: a person's actual subjective expectation of privacy, and the objective reasonableness of such an expectation. Recently, the Court has sought to apply this analysis to electronic surveillance when addressing government installed tracking devices.[63]

If courts fully understand how cell phones work and how they are used, they must conclude that users have no reasonable expectation of privacy in connectivity data generated by their cell phones, whether they are used in public or private places. Modern cell phones connect automatically to various carriers and devices with minimal user interface. Users expect that their devices connect to cellular networks at all times to make and receive calls. While they may not be fully aware of how much data is shared with their carriers to obtain this connectivity, they have actual knowledge of multiple aspects of their devices' data sharing. They know that their devices clearly and constantly demonstrate current levels of connectivity (shown as bars on the cell phone display). Furthermore, users sign terms of service agreements as a condition of use. These not only describe what kinds of information are generated by their phones and provided to their carriers, but also inform them that this data may be provided to law enforcement.[64] Federal Communications Commission regulations regarding E-911 also require that all cell phones provide location data to their carriers to assist in determining the location of calls for emergency service.[65]

Furthermore, in addition to cellular data, smartphones automatically communicate with cellular carriers to establish and maintain Internet connectivity. This results in the automatic provision of additional device connectivity data to third

parties, including enhanced geolocation information.[66] None of this connectivity requires much in the way of user input. Smartphones that are Wi-Fi enabled also automatically seek out Wi-Fi hotspots and determine their availability to provide Internet connectivity. This dialogue results in the automatic sharing of additional data between these devices.[67] Similarly, when a person uses the Internet function on their smartphones to view web pages, a variety of additional, non-content, routing, and signaling information is provided to their carrier and Internet Service Provider (ISP), or to the Wi-Fi hotspot. The majority of courts that have examined this issue have concluded that because of the way in which computers share information to communicate over the Internet, there is no reasonable expectation of privacy in this connectivity data.[68]

In addition, smartphone users often install applications (apps) which cause the device to automatically connect with and send data to app providers. For example, Google, which manufactures smartphones, and Android, a popular cell phone operating system, offers a service called "Google Now." The app, pre-installed on certain Android devices and available for download on Apple devices, performs a variety of automatic functions.[69] It provides real time traffic information based on the user's location, and provides reminders regarding travel and other calendar events. It performs these functions by automatically determining the device's location, and by examining the content of the user's Gmail, contacts and calendars, as well as web browsing history affiliated with the user's Google account.[70] The user consents to this activity by acknowledging Google's terms of service, which state, in part, that Google will collect:

> *Information you give us.* For example, many of our services require you to sign up for a Google Account. When you do, we'll ask for personal information, like your name, email address, telephone number or credit card. . . . [W]e might also ask you to create a publicly visible Google Profile, which may include your name and photo.
>
> *Information we get from your use of our services.* We collect information about the services that you use and how you use them, like when you watch a video on YouTube, visit a website that uses our advertising services, or view and interact with our ads and content. This information includes:
>
> *Device information*
> We collect device specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number). Google may associate your device identifiers or phone number with your Google Account.
>
> *Log information*
> When you use our services or view content provided by Google, we automatically collect and store certain information in server logs. This includes:
> - details of how you used our service, such as your search queries,
> - telephony log information like your phone number, calling party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls.
> - Internet protocol address.
> - device event information such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL.
> - cookies that may uniquely identify your browser or your Google Account.
>
> *Location information*
> . . . [W]e may collect and process information about your actual location. We use various technologies to determine location, including IP address, GPS, and other sensors that may, for example, provide Google with information on nearby devices, WiFi access points and cell towers.
>
> *Unique application numbers*
> Certain services include a unique application number. This number and information about your installation . . . may be sent to Google when you install or uninstall that service or when that service periodically contacts our servers, such as for automatic updates.[71]

It should be noted that the above information is in addition to information provided by the device to the carrier or ISP, in order to connect with Google. Upon request, users can obtain a monthly activity report that categorizes all of the data Google has accumulated on their activity, including a complete tracking record of all phone movements. Google users can log onto their "Google Dashboard" and see a complete record of their movements over the years that Google has maintained data on the tracked device. Dashboard also provides information about browsing history, e-mail and contacts.[72]

Additionally, both iPhone[73] and Android[74] operating systems offer "Find My Phone" features, which allow users to track, with a reasonable degree of precision, the exact geographic location of their phones. This function is enabled through the phone's geolocation tracking capability as it shares location data with Apple and Google. The popularity of these functions is further evidence of the general population's awareness of their devices' automatic connectivity.[75]

Furthermore, as part of the Internet of Everything, cellular devices use Bluetooth technology to communicate with other devices. Bluetooth is a short range radio-based technology that enables devices, such as cell phones, speakers, automobiles, fitness bands, and computers, to communicate.[76] For example, fitness trackers such as Fitbit track physical activity, sleep duration, geolocation of activity, and heart rate. This data is then sent, via Bluetooth, to the smartphone, which transmits the information to Fitbit servers via cellular or Wi-Fi connections. The Fitbit app queries the Fitbit servers and provides users real time reports on their daily physical activity, as well as a historical report on activity and health trends over a period of time. Fitbit also sends users a weekly report regarding trends in data collected.[77]

In sum, modern cell phone users automatically provide a host of connectivity data to multiple third parties. (This

massive volume of shared data is in addition to the content of their phone calls, text messages, and web searching.) Starting with *U.S. v. Miller*,[78] and *Smith v. Maryland*,[79] courts have long recognized that users of communication services have lost any reasonable expectation of privacy in connectivity data shared with multiple service providers.[80] Courts have specifically held that the automated sharing of data over the Internet destroys any expectation of privacy. For example, the Fifth Circuit recently joined the Third, Fourth, Eighth and Tenth Circuits in holding that persons have no expectation of privacy in IP addresses that are shared in the normal course of Internet use.[81] Additionally, courts have ruled that if persons install computer software, such as peer-to-peer file sharing programs, that disseminate child pornography, they have lost any expectation of privacy when they share content as well as connectivity data.[82]

A number of federal courts have recognized that, given current levels of connectivity in our society, courts should not recognize a reasonable expectation of privacy in this cell phone data. In *In re Smartphone Geolocation Application Data*, federal authorities were searching for the target of a pill mill investigation.[83] An arrest warrant was issued and the subject refused to surrender, and authorities did not know where he was. Federal agents applied for an order under the Pen/Trap Statute and the SCA, and a warrant under Rule 41(c) to obtain prospective cell-site location data. In concluding that there was no reasonable expectation of privacy in the routine provision of geolocation data to cellular providers, the court also noted the inherent connectivity of cell phone devices and installed apps.[84] The court also noted that users acknowledge this data sharing in terms of service agreements.[85] The court noted that if users did not want and accept this automatic sharing of data, they could opt out by turning off their phones.[86] In *In re Application of the U.S. for Historical Cell Site Data*, the Fifth Circuit rejected the ACLU's argument that cell phone users retain some expectation of privacy in CSLI whenever they use their phones.[87]

IV. The Way Forward

Until courts demonstrate a greater understanding of the level of connectivity of cell phones and other devices, and this connectivity's impact on legitimate expectations of privacy in the Internet of Everything, they will continue to struggle in applying traditional Fourth Amendment jurisprudence to existing and developing technology. Courts have struggled with the reasonable expectation standard in a variety of other related circumstances. Do persons have a greater expectation of privacy when the government surveillance is conducted in a home rather than a public place? Does the government's use of certain technologies constitute a trespass into a protected area?[88] Does someone who purchases a cell phone using a stolen credit card have any reasonable expectation of privacy in its subsequent use? Do persons have a reasonable expectation of privacy in connectivity data created by stolen phones? Does the right of privacy in historic CSLI differ from that in prospective CSLI? Are there limits to warrantless searches of electronic devices?[89] Are there limits to government's use of high technology devices not available to the general public?[90]

These questions are harbingers of issues to come. As Justice Alito observed in *U.S. v. Jones*, "[t]he availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements."[91] To the extent a person has any reasonable expectation of privacy in simple cellular communication connectivity, does that expectation become unreasonable when the user has an Internet enabled smartphone that is also constantly connecting to cell sites and Wi-Fi hotspots and, at a minimum, sharing location data with them? To the extent that this expectation is reasonable, does it become unreasonable when the smartphone also connects to apps that constantly track the user's location for commercial purposes, or to apps which share highly personal medical data with third parties? If each of these factors changes the degree to which society will recognize an expectation of privacy, how is law enforcement going to know the level of connectivity of the user when making an application for a court order or warrant to search for a particular device?[92]

Finally, because of the growing unwillingness of service providers to provide assistance to law enforcement, even with court orders and search warrants, will the government engage in the greater development and use of self-help surveillance technology such as StingRay to obtain data directly from devices? Two recent cases demonstrate this growing tension.

In a recent case dealing with Microsoft,[93] law enforcement sought the contents of a Hotmail account maintained by Microsoft under the search warrant authority of the SCA.[94] (Microsoft reports that it processes thousands of such requests from federal, state and local authorities.)[95] Microsoft sought to avoid compliance with the search warrant on the novel theory that the servers housing the e-mail were located in Ireland, and that the federal government would have to go through diplomatic channels with the Irish government to obtain the data. The lower courts rejected this argument, and the matter is now awaiting a decision by the Second Circuit.[96] Microsoft seems to be playing a game of Three Card Monte with the data in a cloud computing environment in order to avoid meeting its obligations under the SCA. The essence of cloud computing is the flexibility it gives to storage providers by moving stored data to a variety of storage environments and locations, with the assurance to the customer that the data can be produced anywhere on demand. Microsoft is fully aware that requesting data through diplomatic channels will require months, if not years, of delay in responding to any request where a court has determined that there is probable cause to believe that a crime has been committed and evidence of the crime is in a Hotmail account.[97] There is a question whether Microsoft is truly motivated by a desire to adhere to diplomatic precedent, or merely trying to avoid the cost of compliance with legitimate law enforcement requests.[98] An additional concern is that, if Microsoft loses this case, they could further seek to avoid compliance by moving the data to another jurisdiction where the U.S. has no treaty relations. As noted by the lower court, major service providers are exploring the creation of "server farms at sea," beyond the jurisdiction of any nation.[99]

The Microsoft fight has been eclipsed by the current struggle between the FBI and Apple over unlocking the iPhone used by ISIS adherents in the San Bernardino shooting. Under the authority of the All Writs Act,[100] the DOJ sought to compel Apple to assist in unlocking the phone. Citing First and Fifth

Amendment rights, Apple refused to comply with a court order directing their cooperation. (Apple has also refused to comply with other state and federal court orders for similar assistance.)[101] Many of the service providers that are supporting Microsoft in its fight announced their intention to file amicus briefs supporting Apple.[102] In its pleadings, the DOJ asserted that Apple's intransigence was driven less by a desire to protect privacy, and more by a desire to protect its commercial name.[103] While the DOJ has now sought the dismissal of the San Bernardino All Writs Act matter, because the FBI has been able to access the phone without Apple's help, the struggle to compel Apple to help in other cases is likely to go on.

The privacy bar has sought to portray the use of StingRay devices as an unreasonable encroachment by the government upon Fourth Amendment rights regarding electronic communications. As set forth above, this characterization is not consistent with recognized jurisprudence regarding reasonable expectations of privacy. Instead, the debate should be focused on whether or not there is a need to create a new statutory right of privacy in this area, along with appropriate controls on government access to this data. Some courts have suggested that these and other privacy issues relating to electronic communications in the twenty-first century are best resolved through legislative rather than judicial actions.[104] Through the passage of ECPA, the Pen/Trap Statute, and the Communications Assistance to Law Enforcement Act,[105] Congress has previously demonstrated that it can define non-constitutional rights and controls over government surveillance, and dictate actions which service providers must take to provide assistance to law enforcement. It remains to be seen if Congress is up to today's challenge.

Endnotes

1 No. 15-CF-322, DC Court of Appeals.

2 Spenser Hsu, *Constitutionality of StingRay use by DC police is challenged*, Washington Post (Feb. 24, 2016), *available at* https://www.washingtonpost.com/local/public-safety/constitutionality-of-stingray-use-by-dc-police-is-challenged/2016/02/23/d197cb52-d9b2-11e5-81ae-7491b9b9e7df_story.html.

3 "StingRay" is the most common name of the device manufactured by the Harris Corporation. Other versions of the technology are known as "TriggerFish," IMSI catcher, digital analyzer, "KingFish," "Hailstorm," and cell-site simulator.

4 Information provided includes International Mobile Subscriber Identity (IMSI) information, and Electronic Serial Numbers (ESN), embedded in the device by its manufacturer. Additionally, limited geolocation information is transmitted. This geolocation function is separate from any GPS-related communications.

5 Despite the FBI's attempts to maintain secrecy regarding the existence and capabilities of StingRay technology, one of the most frequently cited documents describing the capabilities of the device is the Department of Justice's (DOJ) 2005 Electronic Surveillance Manual, *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf.

6 18 U.S.C. § 3121-3127.

7 18 U.S.C. § 2703(d).

8 18 U.S.C. § 2510(12).

9 18 U.S.C. § 2510-2522.

10 An "air card" is a mobile hot spot that allows a Wi-Fi enabled device, (e.g., laptop or smartphone) to establish Wi-Fi connectivity via a cell tower. *See, e.g.*, *U.S. v. Rigmaiden*, 844 F. Supp.2d 982 (D. Ariz. 2012). With respect to smartphones, this connectivity is in addition to cellular technology.

11 *See Stingray Tracking Devices: Who's Got Them?*, ACLU, *available at* https://www.aclu.org/map/stingray-tracking-devices-whos-got-them#agencies.

12 *Id.*

13 *See* Henry Bernstein, *The Need for Fourth Amendment Protection from Government Use of Cell Site Simulators*, 56 Santa Clara L. Rev. 177, 194 (2016).

14 *See StingRay Tracking Devices*, ACLU, *available at* https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices.

15 *See* Linda Lye, *Stingrays: The Most Common Surveillance Tool the Government Won't Tell You About*, ACLU of Northern California (2014), *available at* https://www.aclunc.org/publications/stingrays-most-common-surveillance-tool-government-wont-tell-you-about.

16 *See* In re Application of the United States for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer, 885 F. Supp. 197 (C.D. Cal. 1995).

17 18 U.S.C. § 3121-3127.

18 18 U.S.C. § 3122(b)(2).

19 *See, e.g.*, In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 707 F.3d 283, 287 (4th Cir. 2013).

20 442 U.S. 735 (1979).

21 *See* William Curtis, *Triggering a Closer Review: Direct Acquisition of Cell Site Location Tracking Information and Argument for Across Statutory Regimes*, 45 Colum. J.L. & Soc. Probs., 139, 147 (2011).

22 18 U.S.C. § 2703(d).

23 *See* Bernstein, *supra* note 13, at 182-3.

24 *See, e.g.*, Curtis, *supra* note 21; and Bernstein, *supra* note 13. *See also* Stephanie Pell & Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap*: *What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 Yale J.L & Tech. 134 (2014).

25 *See* Bernstein, *supra* note 13, at 174.

26 *See, e.g.*, U.S. v. Rigmaiden, 2013 WL 1932880 (D. Ariz. 2013); *I*n re Application of the U.S., 890 F. Supp. 3d 747 (S.D. Tex. 2012); In the Matter of an Application of the U.S. for an Order Relating to Telephones Used by Suppressed, No. 15-M-0021 (N.D. Ill. 2015) (unpublished opinion); U.S. v. Espudo, 954 F. Supp. 2d 1029, (S.D. Cal. 2013).

27 Historic data is CSLI previously captured and maintained by carriers for their business purposes related to billing and system efficiency. Prospective data is the carrier's real time capture and provision of CSLI to the government to allow the government to determine where the cell phone and its user are located and moving.

28 *See* In re Application of the U.S. for an Order Directing a Provider of Electronic Communications Service to Disclose Records to the Government, 620 F. 3d 304 (3d Cir. 2010) (historic CSLI sought under the Pen/Trap Statute).

29 U.S. v. Graham, 796 F. 3d 332 (4th Cir. 2015) (historic CSLI sought under the SCA).

30 U.S. v. Graham, 2015 WL 6531272 (4th Cir. 2015).

31 *See* In re Application of the U.S. of America for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).

32 *See* U.S. v. Skinner, 690 F. 3rd 772 (6th Cir. 2012) (prospective CSLI).

33 U.S. v. Davis, 754 F. 3d 1205 (11th Cir. 2014) (historic CSLI sought under the SCA).

34 U.S. v. Davis, 785 F. 3d 498 (11th Cir. 2015) (*en banc*).

35 *See supra* note 26, slip op. at pp. 8-10. These controls included steps to reduce overcollection, destruction of overcollected data, restrictions on subsequent use. These controls are already required by the Pen/Trap Statute. 18 U.S.C. §§ 3121(c), 3126.

36 *See id.* at p. 1.

37 844 F. Supp. 2d 982, 996 n.6 (D. Ariz. 2012).

38 442 U.S. 735 (1979).

39 18 U.S.C. § 2701-2712.

40 425 U.S. 735 (1976).

41 12 U.S.C. § 3401, *et. seq*.

42 *See* Letter from Senators Patrick Leahy and Charles Grassley to Attorney General Eric Holder and Secretary Jeh Johnson of the Department of Homeland Security, (Dec. 23, 2014), *available at* http://www.grassley.senate.gov/sites/default/files/news/upload/2014-12-23%20PJL%20and%20CEG%20to%20DOJ%20and%20DHS%20%28cell-site%20simulators%29.pdf.

43 *See* DOJ Policy Guidance: Use of Cell-Site Simulator Technology (2015), *available at* http://www.justice.gov/opa/file/767321/download.

44 *Id.* at 6-7.

45 For example, many federal Offices of Inspector General have law enforcement functions not directly governed by Attorney General Guidelines. In 2002, Congress authorized full law enforcement authority (*i.e.*, authority to make arrests, apply for search warrants, and carry firearms) for many of these organizations on the condition that they agreed to be bound by all Guidelines. *See* Attorney General Guidelines for Offices of Inspectors General with Statutory Law Enforcement Authority (2003), *available at* https://www.ignet.gov/sites/default/files/files/agleguidelines.pdf.

46 The Deputy Secretary of DHS issued a DHS policy statement which mirrors the DOJ policy. *See* DHS Policy Directive 047-02, Department Policy Regarding the Use of Cell-Site Simulator Technology (2015), *available at* http://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators. The policy directive is addressed to DHS law enforcement agents at Customs & Border Protection, U.S. Secret Service, Immigrations & Customs Enforcement, Transportation Security Administration, U.S. Coast Guard, and the Federal Protective Service. *See also* Letter from IRS Commissioner John H. Koskinen to Sen. Ron Wyden (2015) (agreeing that the IRS-Criminal Investigations Division will adhere to the DOJ policy), *available at* http://www.wyden.senate.gov/download/?id=6c9cd25c-28d1-4cda-9199-04a15c0b5d33&download=1.

47 *See, e.g.*, California Electronic Communications Privacy Act, S.B. 178, effective October 2015.

48 *See* Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 Harv. J. L. & Tech. 1, 35 (2014).

49 *See, e.g.*, Letter from FBI Acting Assistant Director, Operational Technology Division to Police Commissioner, Baltimore Police Department and State's Attorney, Baltimore County, (July 13, 2011), *available at* http://s3.documentcloud.org/documents/1808819/baltimore-police-stingray-non-disclosure-agreement.pdf.

50 *Id.*

51 *See* Jason M. Weinstein, William L. Drake, Nicholas P. Silverman, *Privacy vs. Public Safety: Prosecuting and Defending Criminal Cases in the Post-Snowden Era*, 52 Am. Crim. L. Rev. 729, 742 (2015).

52 *See* In the Matter of an Application of the U.S. for an Order Relating to Telephones Used by Suppressed, *supra* note 26 at 2.

53 *See, e.g.*, Office of the Treasury Inspector General for Tax Administration Operations Manual, Chapter 400-Investigations, Section 170.10.2, October 1, 2009, *available at* https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=54&ved=0ahUKEwjanbuOlJPLAhWDRCYKHYKOAig4MhAWCC4wAw&url=https%3A%2F%2Fwww.treasury.gov%2Ftigta%2Ffoia%2Fefoia-imds%2Fchapter400-inv%2F400-170%2Fchapter400-170.doc&usg=AFQjCNF_rM2Jb5OjjCbb3nzrtJWvlBfttw&sig2=hqdg-m9sqa5aW8I52EIXsg&bvm=bv.115277099,d.eWE.

54 18 U.S.C. § 3121(c).

55 18 U.S.C. § 3126.

56 *See* Memorandum of Deputy Attorney General (May 24, 2002), *available at* http://www.justice.gov/sites/default/files/dag/legacy/2007/10/09/memo-05242002.pdf.

57 *See* DOJ Guidance: Use of Cell-Site Simulator Technology, *supra* note 40, at p.6.

58 Court orders for historic cell tower dumps are usually sought under the SCA, 18 U.S.C. § 2703(d).

59 *See* Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. Pa. J. Const. L. 1 (2013).

60 *See, e.g.*, In the Matter of the Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(c) and 2703(d) Directing AT&T, Sprint,/Nextel, T-Mobile, Metro PCS and Verizon Wireless to Disclose Cell Tower Log Information, 42 F. Supp.3d 511 (S.D.N.Y. 2014).

61 *See* In the Matter of Application for Cell Tower Records under 18 U.S.C. § 2703(d), 90 F. Supp. 3d 673, 678 (S.D. Tex. 2015).

62 389 U.S. 347, 361 (1967) (Harlan J. concurring). While Justice Harlan is given credit by scholars for enunciating the two-part test, the majority opinion contains similar guidance: "What a person knowingly exposes to the public, even in his home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* at 351-52 (citations omitted).

63 *See* U.S. v. Jones, 132 S. Ct. 945, 950 (2012).

64 *See* In re Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 141-142 (E.D.N.Y. 2013).

65 *See* 47 CFR §20.18(h).

66 In addition to geolocation data provided to carriers, such as Verizon and AT&T, smartphones may also provide significant location information to app service providers, such as Apple and Google, to enable enhanced mapping and location services provided by these devices. *See* Sean Gallagher, *Where've you been? Your smartphone's Wi-Fi is telling everyone*, ArsTechnica (Nov. 5, 2014), *available at* http://arstechnica.com/information-technology/2014/11/where-have-you-been-your-smartphones-wi-fi-is-telling-everyone/.

67 *See* Dan Goodin, *Loose-lipped iPhones top the list of smartphones exploited by hacker*, ArsTechnica (March 16, 2012), *available at* http://arstechnica.com/apple/2012/03/loose-lipped-iphones-top-the-list-of-smartphones-exploited-by-hacker/.

68 *See, e.g.*, U.S. v. Forrester, 512 F.2d 500, 510 (9th Cir. 2007) ("Internet users have no expectation of privacy in the . . . IP address of the websites they visit because they should know that this information is provided to and used

by Internet service providers for the specific purpose of directing the routing of information.")

69 *See, e.g.*, Whitson Gordon, *Top 10 Awesome Features of Google Now*, Lifehacker (May 17, 2014), *available at* http://lifehacker.com/top-10-awesome-features-of-google-now-1577427243.

70 One researcher has estimated that, as of December 2015, 100-200 million of the estimated 1.4 billion Android users are currently using Google Now. *See* Shushant Shekar, *How Many People Are Currently Actively Using Google Now?*, Quora (Dec. 25, 2015), *available at* https://www.quora.com/How-many-people-are-currently-actively-using-Google-Now.

71 *See* Google Privacy Policy (Aug. 19, 2015), *available at* http://www.google.com/policies/privacy/ (privacy policy applies to all Google services, not just Google Now).

72 *See Your Timeline: Revisiting the world that you've explored*, Google Maps Blog (July 21, 2015), *available at* https://maps.googleblog.com/2015/07/your-timeline-revisiting-world-that.html; Google Dashboard, Google Privacy Youtube Channel (Nov. 4, 2009), *available at* https://www.youtube.com/watch?v=ZPaJPxhPq_g#t=48.

73 *See* Find My iPhone, iTunes App Store, *available at* https://itunes.apple.com/us/app/find-my-iphone/id376101648?mt=8.

74 *See* Find My Lost Phone!, Google Play App Store, *available at* https://play.google.com/store/apps/details?id=com.fsp.android.phonetracker&hl=en.

75 For example, according to the Google Play Store, over 220,000 users have reviewed the Android Find My Lost Phone! App, giving it an average of four stars out of five. *Id.*

76 *See* Bluetooth Technology Basics, *available at* https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics.

77 *See* How do Fitbit trackers sync their data?, *available at* https://help.fitbit.com/articles/en_US/Help_article/How-do-Fitbit-trackers-sync-their-data.

78 425 U.S. 735 (1976).

79 442 U.S. 735 (1979).

80 *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561 (2009).

81 *See* U.S. v. Weast, No. 14-11253, slip op. at 4 n.10. (5th Cir. 2016).

82 *Id.* at n.11.

83 *Supra* note 64.

84 *Id.* at 138-141.

85 *Id.* at 147.

86 *Id.* at 146.

87 724 F. 3d 600, 613-614 (5th Cir. 2013). *See also* U.S. v. Guerrero, 769 F. 3d 351 (5th Cir. 2014), *cert. denied*, 135 S. Ct. 1548 (2015).

88 *See Jones*, *supra* note 63 at 953 (government's physical intrusion to install surveillance technology may violate Fourth Amendment, but trespass is not the exclusive test to determine if there has been a search).

89 *See* Riley v. California, 573 U.S. __, 134 S. Ct. 2473 (2014), where the Court ruled that a warrantless search incident to arrest of the contents of a cell phone was improper, when that search sought information not related to the cause of the arrest.

90 *See* Kyllo v. U.S., 533 U.S. 27 (2001).

91 *Jones*, *supra* note 85 at 963 (Alito, J., concurring).

92 These questions differ from the cell phone issues recently confronted by the Court in *Riley*. There the court ruled that the government will need a warrant to search the content of a cell phone incident to arrest, when the search is targeted at information not related to the crime of arrest. In reaching this decision, the court noted that modern cell phones are ubiquitous, carry massive amounts of data, and carry much information related to the daily lives of users. This relates to the *content* on cell phones, not their *connectivity*. In creating a higher privacy standard requiring a warrant to obtain content, the Court did not examine the fact that these devices automatically share massive amounts of connectivity data. This sharing of data with third parties is a significant alteration of the *Riley* analysis and conclusion. Courts which have subsequently examined the issue have refused to extend *Riley*'s holding to CSLI. *See*, *e.g.*, U.S. v. Guerrero, *supra* note 87.

93 *See* In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, No. 14-2985 (2d Cir. 2015).

94 18 U.S.C. §2703(a).

95 *See* Law Enforcement Request Report 2015, at 2, *available at* https://www.microsoft.com/about/business-corporate-responsibility/transparencyhub/lerr/.

96 *See* In re Warrant to Search a Certain E-Mail Account, 15 F. Supp. 3d 466 (S.D.N.Y. 2014).

97 *See* Statement of David Bitkower, Principle Deputy Assistant Attorney General, DOJ, Before House Judiciary Committee (Feb. 25, 2016), *available at* http://judiciary.house.gov/_cache/files/c8d735e5-c9ab-4197-ac76-2c6f5d4b03cd/doj-bitkower-testimony.pdf.

98 Microsoft is not alone in opposing this warrant. Other major online service providers, such as Amazon, Apple, AT&T, and Verizon have filed amicus briefs supporting Microsoft.

99 *See* In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by the Microsoft Corporation, 15 F. Supp. 3d 466, 475 (S.D.N.Y. 2014).

100 28 U.S.C. § 2651.

101 *See* Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance, ED No. CM-16-10 (Feb. 25, 2016), *available at* http://www.nytimes.com/interactive/2016/02/25/technology/document-apple-motion-opposing-iphone-order.html.

102 *See* Ellen Nakashima, *Google, Facebook and Other Powerful Tech Firms Filing Briefs to Support Apple*, Washington Post (Feb. 29, 2016), *available at* https://www.washingtonpost.com/world/national-security/google-facebook-and-other-powerful-tech-firms-filing-briefs-to-support-apple/2016/02/28/beb05460-de48-11e5-846c-10191d1fc4ec_story.html?hpid=hp_rhp-more-top-stories_no-name%3Ahomepage%2Fstory.

103 *See* Government's Motion to Compel Apple Inc. to Comply with This Court's February 16, 2016 Order Compelling Assistance, ED No. CM-16-10 (Feb. 19, 2016), *available at* http://apps.npr.org/documents/document.html?id=2716063-Apple-iPhone-Access-MOTION-to-COMPEL.

104 *See* In the Matter of an Application of the U.S. for an Order Authorizing Disclosure of Location Information of a Specific Wireless Telephone, 849 F. Supp. 2d 526 (D. Md. 2011), in which a magistrate judge concluded that neither the Pen/Trap Statute, the SCA, Rule 41, nor the All Writs Act provided sufficient authority to require carriers to produce prospective CSLI when the government could not establish that the target was aware of his fugitive status on outstanding charges. The court concluded that such authority has not yet been provided by Congress.

105 47 U.S.C. § 1002(a)(2).