

Identifying Law Enforcement Needs for Access to Digital Evidence in Remote Data Centers

Michael J. D. Vermeer, Dulani Woods, Brian A. Jackson

Key Findings

- Expert panelists on the acquisition and use of digital evidence and on relevant law and technical issues convened to discuss challenges associated with law enforcement requests for digital data held in remote data centers. The panelists identified 36 needs for mitigating those problems.
- Participants highly ranked needs related to facilitating better communication and understanding between law enforcement and service providers. These needs included calls for information exchanges for points of contact and on the types of data held by service providers, devices, and apps. Participants acknowledged that there is often an adversarial relationship between law enforcement and providers and discussed means of developing a shared perspective and improving cooperation.
- Highly ranked needs also included better investigator access to information and training on requesting remote digital evidence. Several needs recommended creating databases and portals from which practitioners could exchange documentation and access standardized online training and best practices. Other needs called for the development of better standards for serving legal process and incentivizing research communities to keep methodologies for digital evidence acquisition current.
- Participants identified several needs related to improving the MLAT process and ranked most of these needs in the upper-middle tier. Participants largely agreed that the current state of the MLAT process is inadequate to meet the growing need for law enforcement access to extraterritorial digital evidence. Specific MLAT-related needs included the creation of an online docketing system, research and analysis on MLAT data to identify bottlenecks, the development of a uniform system of jurisdiction, better training and information for U.S. trainers of foreign nationals on U.S. law, and research on expanding the MLAT regime to cover current gaps.

Law enforcement increasingly needs to have access to data residing in remote data centers, and investigators frequently face multiple barriers in this process. As more data routinely collected by investigators have come to reside in remote locations, these barriers have become a growing challenge for stakeholders.

On behalf of the National Institute of Justice (NIJ) and as part of the Priority Criminal Justice Needs Initiative, the RAND Corporation, in partnership with the Police Executive Research Forum, organized a workshop in May 2017 on Challenges with Law Enforcement Access to Digital Evidence Held in Remote Data Centers. The workshop brought together experts on the acquisition and use of digital evidence and on relevant law and technical issues from around the United States to discuss challenges associated with law enforcement requests for digital data held by third parties that may reside across state or national boundaries. Discussions focused on ambiguities in U.S. law and procedure, challenges associated with using the Mutual Legal Assistance Treaty (MLAT) process, issues stemming from inadequate cooperation between law enforcement and service providers (the companies and organizations providing remote storage, communication, and computing services), and technical issues related to evidence residing in the cloud.

During the workshop, participants discussed specific problems they faced and identified 36 needs for mitigating those problems. *Needs*, in this case, are the means of solving a key problem or improve performance over the baseline. As such, a *need* includes both a problem or an opportunity, as well as a related solution or innovative idea. Following this discussion, the needs were prioritized using the Delphi Method to produce a ranked list of high-priority needs (RAND Corporation, 2017). The highest-priority needs revolved around the creation of information exchange systems, better online training and standards, and incentives

for researchers to keep the knowledge base current on methodologies for acquiring digital evidence. Multiple highly ranked needs also called for improvements in the MLAT process, such as efforts to make the process more transparent or make more information on the process available. The ranked list of needs will help decisionmakers prioritize effort and funding to improve the processes for law enforcement access to digital evidence for all stakeholders involved.

INTRODUCTION

Requests for Remotely Held Digital Evidence

Consider the following scenario: A man searches for an item on Craigslist and discovers a potential seller. The buyer and seller communicate via a texting app and arrange to meet to complete the sale. Near the spot where the two had arranged to meet, the buyer is assaulted, robbed, and killed. Later, the officer investigating the crime discovers that the buyer was on his way to meet a Craigslist contact, finds out that there was a text conversation between the two, and obtains a warrant from a local judge to request the content of the conversation from the service provider. After making the request, however, the officer does not receive a reply within a month. When the provider finally responds, the response is a refusal to comply, citing a lack of jurisdictional authority for the local judge to issue a warrant on data held by the provider several states away. The officer then spends some time finding the appropriate contacts to aid in the legal process for requesting the data in the provider's local jurisdiction. Upon issuing the new request to the provider, the officer waits another month before receiving a reply. When the provider supplies the requested data, they are in a format that is unreadable without special software, further delaying the investigative process while the officer attempts to find the information needed for the investigation. Several months have passed since the murder.

In another example, consider an officer investigating a child exploitation case. The officer has reason to believe that a suspect is using a cloud storage account to perpetrate a crime. The cloud storage provider is given a data preservation notice for the suspect's data and the officer obtains a warrant to retrieve the data. After being served the request, the provider only partially complies: Portions of the data are stored overseas and the provider claims that it is outside of the authority of U.S. law enforcement to request them. Knowing that a request through

an MLAT would be required to obtain the data (likely meaning many months of waiting, a significant coordination burden for the officer, and an uncertain result), the officer sees no option but to abandon pursuit of the extraterritorial data, to the evidentiary detriment of the case. Meanwhile, although the data held by that particular provider are preserved, the provider notifies its subscribers of a law enforcement investigation involving its services. The suspect is thus made aware of the investigation and is able to access similar services he uses and delete incriminating evidence. When officers later discover and access these other accounts, the evidence is gone, and, unlike in some other digital storage media, technical aspects of these service providers' cloud storage architectures render the deleted data unrecoverable. Finally, the suspect is eventually brought to trial, and the lawyer for the defense impugns the trustworthiness of the evidence from the cloud by noting the forensically unsound manner in which the cloud service provider (CSP) preserved and delivered it. The prosecutor has insufficient technical expertise with cloud-derived data to effectively rebut the defense's argument. Ultimately, the available evidence that law enforcement was able to obtain proves insufficient to convince the jury, and the suspect is acquitted.

These are notional examples meant to illustrate the problems regularly faced by law enforcement when seeking data held in remote data centers, but other high-profile cases have recently been fought that share many of the same challenges, most notably the 2014 case of *Microsoft v United States*, also known as the *Microsoft Ireland* case (Blanco, 2017), and recent cases involving Google (Memorandum of Decision, 2017; Fox-Brewster, 2017). In the *Microsoft Ireland* case, Microsoft successfully had a warrant quashed that had compelled the company to provide emails stored on a server in Ireland. The case is currently being reviewed by the U.S. Supreme Court. In the Google case, Google had used the process of "sharding" to store portions of files on its cloud servers in various places, including in other countries. In this case, it unsuccessfully argued that, because portions of these files resided in other countries, it could not be compelled with a warrant to produce the related data. These conflicting cases concern the authority, as stated in current law, of the U.S. government to compel disclosure of digital evidence held by providers across state and national boundaries. The cases have yet to fully clarify this authority with respect to recent technological changes. Meanwhile, while remotely stored data proliferate and become more ubiquitous, law enforcement, commercial providers, and users alike operate within a challenging and unclear environment where the extent of legal authority and of privacy rights remains murky within U.S. statute.

Digital Evidence Held in Remote Data Centers

The cases and scenarios described earlier illustrate many of the issues with digital evidence held in remote data centers. Some of these issues affect digital evidence generally, but evidence held remotely presents unique concerns that warrant additional attention. These include concerns over conflicts with service providers (the companies and organizations providing remote storage, communication, and computing services), concerns over the territoriality of data, and concerns about technical challenges to evidence collection, analysis, and presentation.

Despite concerns and challenges related to accessing remotely held digital evidence, law enforcement cannot perform its function effectively, in some cases, without that access, and the issues under discussion cannot be ignored without significant negative repercussions. Law enforcement was able to perform its task adequately decades ago, before the existence of digital evidence, because law enforcement had the tools, training, and legal means of tracking and acquiring the evidence that was available at the time. As new technology has allowed people to communicate and leave evidence of crimes committed in different ways, much of the means of committing crimes and the evidence thereof has irrevocably shifted with our shifting approach to digital communication and data storage. Today, nearly every person carries a device that they use to communicate with others multiple times per day and that may store data documenting their activities half a continent away, not to mention myriad other devices that hold evidence of our daily activities in various ways. Law enforcement must be given the tools, legal means, and guidance to adapt effectively to this new reality while safeguarding individual privacy. In various ways that we will discuss, this has not been the case.

Scope

Digital evidence held in remote data centers originates in many places and can take a variety of forms. Cloud computing or storage services are primary examples, but the category of data

under discussion has a much broader scope than merely cloud services. Remotely held digital evidence, for the purposes of this report, comprises any digital information owned, used, or pertaining to an individual that is stored or maintained by a third party at a location remote from the user or customer. The following list aims to provide the categorical scope of remotely held digital evidence with some common examples, but it is by no means exhaustive. Remotely held data can originate from any of the following:

- cloud storage services: Google Drive, Dropbox, email services
- biometric tracking devices: Fitbits and other health trackers
- location trackers: cell phones and other devices with Global Positioning System (GPS) and location services
- presence devices: Amazon Echo, Nest, and other similar devices
- internet of things (IoT) devices: internet-connected locks, lights, and appliances
- messaging services: Kik, Viber, WhatsApp, messaging over gaming consoles.

The data that originate from these places, devices, and services warrant attention as special cases of digital evidence because of a variety of complicating factors, including the involvement of third-party stakeholders, questions of extra-jurisdictional or extraterritorial legal authority, and technical challenges associated with the storage architectures and business models used in remote data centers. Evidence repositories and databases held by such government agencies as the Federal Bureau of Investigation (FBI) are also within the scope of this report. While these are distinct from the items mentioned earlier in that the third party holding the data is also a government agency, law enforcement may face similar challenges with these databases, such as issues with access and connectivity, with locating relevant evidence, and with the awareness of data availability.

Law enforcement must be given the tools, legal means, and guidance to adapt to the new technological reality while safeguarding individual privacy.

Service Providers

Digital evidence in remote data centers is similar to other digital evidence, in that it is usually owned and used by the customer or subscriber. However, unlike other digital evidence, the physical storage medium is owned and possessed by a third party: the service provider. Providers have the incentive to build their storage architectures and business models in such a way as to maximize the efficiency of the system and its effectiveness to the user. Benefits to the user may include such features as heightened security measures and built-in encryption but may not include extensive backups of user data or easy data preservation that could facilitate law enforcement investigations. Additionally, the dynamic nature of remote data storage, where data may be routinely transferred from one location to another, typically precludes subscriber; law enforcement; and, in some circumstances, even the provider from having concrete information on the physical location of stored information.

The nature of remote storage has implications for law enforcement investigations that have need of user data. The lack of information on the physical location of data typically makes it impossible for investigators to follow some common practices in digital forensics, such as the acquisition or imaging of a storage disk. Typically, investigators also will have limited information on the storage environment outside what is given to them by the provider. Investigators are therefore often wholly dependent on providers for data and metadata pertinent to the

The dynamic nature of remote data storage typically precludes subscriber, law enforcement, and even the provider from having concrete information on the physical location of stored information.

investigation. Requests or warrants for data must be made to, and fulfilled by, service providers.

As such, the interaction requires careful and detailed communication between the provider and the officer as to what data the investigation requires, how they must be handled, what the resulting data format should be, what is technically feasible, and various other concerns that take into account burdens on the provider and needs of the investigation. Providers are required to actively supply the information law enforcement requests, rather than passively comply with search and seizure by investigators. Indeed, such requests can prove to be a significant and costly burden to both parties. As such, service providers are not merely inactive third parties or observers of the legal process, but must be viewed as true stakeholders, with interests and rights that must be considered and balanced along with the legitimate investigative needs of law enforcement and the digital privacy rights of individuals.

Governing U.S. Statutes and Rules

While the most relevant document is surely the Fourth Amendment to the U.S. Constitution, which establishes a citizen's right to be secure from unreasonable search and seizure, several U.S. statutes governing privacy rights related to electronic communications and information have also been passed in the past few decades, beginning with the Wiretap Act in 1968, which focused on the telephone. The U.S. Congress amended the Wiretap Act over time, enacting the Communications Assistance to Law Enforcement Act; the Patriot Act; and, most notably, the Electronic Communications Privacy Act (ECPA) (18 U.S. Code [U.S.C.] 2510-22). The applications of these and other statutes to digital evidence writ large was explored in more depth in our previous report on digital evidence (Goodison, Davis, and Jackson, 2015) and, thus, will not be explored further in this report. The ECPA, and in particular, Title II, has direct application to and is of critical importance for digital evidence held in remote data centers.

The ECPA was enacted in 1986 to address issues related to computing technologies that were not covered under the Wiretap Act, and it remains the most relevant statute concerning electronic communications and digital evidence today. The Stored Communications Act (SCA) was enacted as Title II of the ECPA (18 U.S.C. 2701-11). While the Wiretap Act covered protections against real-time access of electronic communications, the SCA aimed to provide protections against access to stored records. The SCA dictates privacy rights for users of two

different kinds of services: electronic communication services (ECSs) and remote computing services (RCSs). Its language applies to the services, not to users, and differing levels of protection are afforded to records held by an ECS provider versus an RCS provider. The SCA prohibits the voluntary disclosure of users' stored communications by these service providers, with some exceptions, and dictates the means by which the government might compel disclosure of user records from these service providers. In general, communications held by an ECS cannot be knowingly and voluntarily divulged to any third party, including government entities, while in electronic storage. Exceptions to this prohibition allow the provider to disclose user communications or records in certain situations, although exceptions are different for communications versus user records (18 U.S.C. 2701-2).

Furthermore, 18 U.S.C. 2703 details the means by which government entities might compel disclosure of various types of communication records, with different legal instruments specified based on the type of record being sought and varying degrees of privacy protection against its search and seizure. Different types of records are afforded varying degrees of privacy protection by requiring provision of notice to the customer whose records are being sought or requiring varying degrees of suspicion of relevance to a criminal investigation, based on "specific and articulable facts," up to and including probable cause. Content records, such as the text of an email, are afforded the greatest degree of protection, requiring a warrant, which may only be issued with probable cause. Noncontent records, such as metadata on the names or Internet Protocol (IP) addresses of senders or recipients, may be obtained with a court order, provided there is reasonable suspicion that the record is relevant to a criminal investigation.¹ Finally, an administrative subpoena can be used to obtain some noncontent information, including means of payment.

These requirements also have an important exception that might allow a government entity to obtain a more stringently protected record with a lesser legal instrument based on the length of time in storage or provider type. Content records held by an ECS for 180 days or less always require a warrant for access. According to the statute, if a record has been held in storage by an ECS for more than 180 days or if it is held by an RCS, content information may be obtained with a court order or an administrative subpoena, provided the customer is

¹ The requirement for reasonable suspicion for access to metadata was added in a 1994 amendment to the ECPA.

notified of the request. However, the notice may be delayed by 90 days if the court determines that notification may have an adverse result. A recent court ruling found, however, that a warrant is required for access to emails, based on Fourth Amendment protections (*United States v Warshak*, 2010). It is also important to note that section 2703 states that a court order for provision of content or noncontent records may be quashed if the provider promptly makes a motion to do so because "the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider." The legal process required for various records under the SCA is summarized in Table 1. Finally, section 2703 specifies a requirement for the provider to preserve evidence for 90 days upon request, with the possibility of an additional 90 days upon renewal.²

Warrants issued for the search and seizure of electronic content records in criminal investigations require probable cause, based on Fourth Amendment protection against unlawful search and seizure. These warrants are issued by magistrate judges with authorities in specified districts. They cover a particular location and thus have an explicitly territorial reach. In practice, warrants based on two categories of stored content are used: those specified in Federal Rule of Criminal Procedure (FRCrP) 41 and those in the SCA. The key difference between the two is that a FRCrP 41 warrant is issued by a magistrate judge for property in each district in which the records are located, whereas an SCA warrant is issued by a magistrate judge in the district in which the crime was committed for a service provider that may reside in another district (Cauthen, 2014). Both FRCrP 41 and SCA warrants are presumed to have authority only within U.S. territory.³

Extraterritorial Evidence

The statute's explicit statement of authority only within U.S. territory is a critical factor when considering law enforcement requests for digital evidence that may be held, in whole or in part, extraterritorially, because there is a presumption against extraterritorial application of U.S. law. Recent court decisions have stated that, without a contrary intent or a clear indication

² For more background on court interpretations of the provisions of the SCA, see Thompson and Cole, 2015.

³ Note that the presumed territorial reach of warrant authority is a key issue in the Microsoft Ireland case, with arguments over whether the territorial warrant authority is based on the location of the provider or the location of the data.

Table 1. Legal Process Required Under the SCA for Various Records

Type of Record	Electronic Storage < 180 Days	Electronic Storage > 180 Days
Content record with ECS	Warrant without notice	Warrant without notice; court order or subpoena with (delayed) notice
Content record with RCS	Warrant without notice; court order or subpoena with (delayed) notice	Warrant without notice; court order or subpoena with (delayed) notice
Noncontent information	Subpoena without notice	Subpoena without notice

that a statute applies extraterritorially, that statute is meant to apply only within U.S. territory and may have no extraterritorial application. This is meant to preserve international comity and prevent unintended clashes between various nations' laws (*EEOC v Arabian American Oil Co.*, 1991). As such, when law enforcement needs evidence stored overseas, the appropriate way to acquire it is to request that the host country compel provision of the evidence with its own legal authority, otherwise known as a request for mutual legal assistance (MLA). This process is possible for those countries with which the United States has an MLAT that dictates terms for sharing evidence between the countries. These partners have agreed through MLATs to participate in government-to-government sharing of data and evidence and to respect the host country's legal process and authority within their borders. This agreement requires sometimes burdensome coordination between countries; a balance of sovereignty interests; and a mutual understanding of laws, authorities, and legal terms. It does, however, provide a means for lawful cooperation across borders and serves to avoid situations where third-party service providers may be caught between the demands of conflicting national laws (Woods, 2015).

Many of the service providers with data held in remote data centers are based in the United States, although there is an increasing number of non-U.S. providers. Even the U.S.-based companies are often transnational and may store all or parts of certain records overseas, introducing complexity into the territorial nature of that data and the legal authority for their disclosure to government entities. The Microsoft and Google cases mentioned earlier illustrate this point.

In This Report

The growth of cloud computing, the remote storage of and access to data, and, especially, the extraterritorial nature of these data, have introduced multiple challenges for law enforcement, privacy advocates, commercial companies, and cyberse-

curity professionals in recent years. While acquisition of remote or extraterritorial evidence has always been cumbersome to some degree, the rise of cloud- and web-based digital services has increased the frequency of data requests and the accompanying burden for all parties involved. State and local law enforcement increasingly see the need to obtain data and digital evidence held extraterritorially or by transnational companies in their investigations of local crimes. The challenges associated with this need are multifaceted, involving legal, procedural, and technical difficulties.⁴

This report builds on a previous report in this series identifying needs related to digital evidence (Goodison, Davis, and Jackson, 2015). The term *needs*, in this case, describes the way to solve a key problem or improve performance over the baseline. As such, *needs* include both a problem or an opportunity, as well as a related solution or an innovative idea. Many of the needs mentioned in the previous report, including examples of issues related to data storage volumes, investigator training, and forensics tools, also are associated with remote digital evidence.

The next section will explore issues and challenges affecting stakeholders. The following section will describe the expert panel discussion held at the NIJ offices in May 2017 to discuss and prioritize needs and solutions to some of these challenges, as well as the results thereof. The final sections present the needs discussed by the panel, ranked by priority, as well as a brief conclusion. The intent of this report is to describe the scope of the challenges, summarize the expert panel's discussion surrounding the issues, and provide a list of needs identified and prioritized by the expert panel that will help inform stakeholders. Ultimately, the goal is to improve law enforcement access to and use of remotely held digital evidence in a manner that is legal, effective, timely, and understandable.

⁴ For another helpful summary of these challenges, see Chertoff Group, 2015.

CHALLENGES WITH DIGITAL EVIDENCE HELD IN REMOTE DATA CENTERS

The characteristics of remotely held digital evidence noted earlier introduce sets of related challenges. Ambiguous and outdated language in the SCA, questions of jurisdictional and territorial reach and authority, and challenges arising from provider involvement in the legal process are just some of the statutory and procedural issues plaguing stakeholders. Technical challenges associated with performing digital forensics on remote data centers, analyzing the data, and presenting them clearly to the court add to these issues. This section will delve into each of these areas in more depth and discuss some proposals for the reform of laws and processes.

Ambiguities in U.S. Law and Procedure

The ECPA was passed in 1986, before the advent of many elements of modern electronic information and communication technology, including the internet, mobile devices, cheap data storage, or cloud computing. As a result, the language used to legislate digital privacy rights and exceptions for compelled disclosure of electronic records for modern technologies in the SCA are ambiguous and outdated.

As mentioned above, the SCA specifies different protections afforded to a record based on a few defined distinctions. It defines differences between content and noncontent records, whether or not a record is held in electronic storage, and whether the record is held by an ECS provider or an RCS provider. It assigns evidentiary requirements needed for government access to records based on these distinctions. This approach is problematic because the definitions of electronic storage, ECS, and RCS were made to apply to a decades-old technological context that has changed significantly: The advances in technology and services offered by today's multifunction providers have blurred the distinctions made in the SCA.⁵

When the law was passed, data storage was expensive, and, presumably, the modern approach to electronic record storage was not foreseen by the crafters of the law. Users now routinely store nearly all their electronic communications indefinitely, providing a record of communications over many years ("How Much is Your Gmail Account Worth?" 2012). Also, users

are separated from their data, often unknowingly, by miles, jurisdictions, and even borders, while retaining instant access to them from a local device. In some cases, providers may intend to store data in specific, distant locations, while in other cases it may simply be a result of technologies or practices intended to store and transfer data most efficiently.

The SCA has a presumed territorial reach, but ambiguity remains over what this means and how the presumption against extraterritorial application applies to data relevant to an investigation. Consider what territorial authorities govern in a given situation: If a crime is committed by a U.S. resident and the evidence of that crime is stored in a server maintained in a foreign country by a provider with facilities that span the globe, what is the appropriate basis for establishing territoriality and legal authority for search and seizure? Arguments could be made for establishing territoriality based on the residency of the suspect, the citizenship of the suspect, the location of the crime, the location of the service provider's headquarters, the location of the data center where the record is maintained, and so forth. Furthermore, should territoriality be established based on data location, the data may traverse borders to another server on a regular basis, or be split into shards that reside in different countries, further complicating the issue. A definitive determination on data territoriality has not been reached, and there is ongoing debate about what should constitute a territorial or extraterritorial action with regard to such data (Daskal, 2015; Woods, 2016).

In addition to struggling with new issues of data territoriality, the law also creates distinctions that were clear at the time of its writing but have since been blurred by new technology, such as the distinction between RCS and ECS providers. Records held by an ECS provider require a warrant for access (when held in electronic storage for 180 days or less), but

Advances in technology and services offered by today's multifunction providers have blurred distinctions made in U.S. law.

⁵ For more in-depth discussion on issues with SCA language, see Thompson and Cole, 2015, and Kerr, 2014.

records held by an RCS can be obtained with a court order or subpoena regardless of storage time. However, modern service providers perform many different functions, each of which could be construed as the functions of an ECS, an RCS, or neither. A single service provider might, for example, offer services that provide text chatting, email, web search functionality, and cloud storage of communications and other user files. This provider might simultaneously act as an ECS provider; an RCS provider; or, occasionally, neither, according to the definitions in the statutes. This multifunctionality of modern providers blurs the distinctions between the two provider types to which the SCA applies, and so confuses both the legal protections afforded to records held by each provider type and the appropriate legal process to compel disclosure (Kerr, 2014).

Law enforcement practitioners seeking data held in the cloud also routinely face a number of challenges with the manner in which data are stored that complicate digital forensic investigations. In addition to issues identified in the previous digital evidence workshop (Goodison, Davis, and Jackson, 2015), such as large data volumes, inadequate forensic tools, and insufficient investigator training, cloud environments and remotely stored digital evidence provide a number of other technical challenges to digital forensics. As discussed earlier, locational uncertainty of data in the cloud can have challenging implications related to jurisdiction and legal authority for law enforcement. It is also a technical challenge because law enforcement seeking access to or seizure of the data, often through a CSP intermediary, can be stymied or delayed when investigators have no technical means of establishing data location. Data multiplicity and distributed storage may mean that the data are physically in many places at once, in part or in whole. While CSPs must at least know when their resources are used, the distributed nature of the cloud architecture may make it practically impossible to determine the physical location of the data (Dykstra, 2013).

In addition to potentially seizing or copying the data and establishing jurisdiction, two beneficial aims in determining data location are the ability to reconstruct the crime and the ability to link the suspect's identity to the actions taken and the devices used. Data and devices that are distributed over geographic areas will have different time zones associated with them and put their own time stamps on the data in their logs. When the locations are not known, correlating the data across multiple sources to create a synchronized timeline and a body of evidence can be very difficult (Alqahtany et al., 2015). Furthermore, cloud environments may have many layers of service

and ownership connected to the user. In the case of Dropbox, for example, the user contracts with the CSP, which is Dropbox. Dropbox provides the service to the user with capacity it obtains from Amazon Web Services, a cloud infrastructure provider. Communication between the user and the cloud services is further facilitated by a communication service provider. If a Dropbox user at one point used Dropbox to store a file containing evidence of a crime, an investigator must first establish the entity on which to serve an information request in order to obtain the needed evidence: Dropbox, the service the individual used; Amazon Web Services, the owner of the server on which the actual file was located; or the communication service provider that handled the transmission of the information. After sorting out ownership and the legal process, the investigator must try to establish a clear timeline of activity, confirming and synchronizing activity and time stamps between the user's local device and one or more of the service providers that clearly link the user to their digital activity. Clearly synchronizing an activity timeline in this manner and establishing a link between the user and the criminal activity across the many devices, services, and owners involved can be extremely challenging (Walden, 2011).

Further complicating matters, various forms of evidence may or may not be retained, depending on the user model and practices of the providers. Various activity logs, registry entries, and temporary internet files may form some of the available digital evidence of a crime. However, the dynamic nature of the cloud environment might make such entities either inaccessible or short lived, depending on the user model. If these data are not stored on a user's local device and if the cloud user model does not include persistent storage capability, they will be unrecoverable when the user ends their session (Taylor et al., 2010). While these temporary data may be lost, some cloud user models do enable imaging of the server or storage space occupied by a user's virtual machine, which may preserve the majority of the evidence. However, even in these cases, the distributed nature of the cloud may introduce complications, as multiple users may have had activity on the same storage space. In this case, because many users have been adding, deleting, and modifying data in the same space, it could be challenging to uniquely attribute some data or activity to the suspect in question or prove that their data were not tampered with. Moreover, seizing the physical storage medium on which multiple users—most of whom are not involved in the alleged crime—have their data stored also introduces privacy concerns (Zawoad and Hasan, 2013).

Ambiguity around data territoriality and jurisdictional authority often forces local crime investigations into the realm of international affairs.

The challenges associated with multiple tenancy on cloud storage are related to a broader theme: trust and authenticity of evidence from the cloud. The integral role of the CSP in the isolation, preservation, collection, and transfer of evidence is a significant factor in this. Consider a digital forensic investigation where all evidence is located on a hard drive or mobile device. Juries will eventually be asked to place trust in, for example, the law enforcement investigator, the tools they used to examine the devices, the security and trustworthiness of the device storage systems, and the maintenance of proper chain of custody. When evidence resides in the cloud, however, the trust that is required expands significantly. Now trust is required in the distributed architecture (which is often opaque to investigators) to accurately store, partition, and reassemble the data; in the integrity of the many layers of operating systems and communication channels; in the technicians tasked to assemble and deliver the evidence; and in many others, in addition to the elements of traditional forensics. As a result, investigators must examine data at multiple layers of the cloud architecture and correlate findings across them to reduce risk to the security, authenticity, and trustworthiness of the obtained evidence and then find a way to clearly communicate this activity to a jury of laypeople (Dykstra and Sherman, 2012).

Finally, the priority for the CSP will often be to minimize disruption to its business, rather than to ensure a forensically sound investigation. It may or may not have personnel trained in forensically sound practices for delivering evidence to law enforcement. CSPs must be relied on to, for example, isolate a cloud incidence to protect data from adulteration or tampering, a requirement that is usually complicated by the multiple user tenancy of cloud storage. Loss of information on how data were collected or stored, an unclear record of the chain of custody, or other ways in which the ownership or quality of the data may be compromised might, at best, make the trustworthiness of the data questionable, and, at worst, make the data inadmissible in court.

The MLAT Process

Issues of jurisdiction and authority have created challenges for both government and private entities. Ambiguity around data territoriality and jurisdictional authority often forces local crime investigations into the realm of international affairs, as investigators must use the MLAT process to acquire extraterritorial data. In most cases, the MLAT process is cumbersome, placing a significant burden on both law enforcement and providers as they encounter more requests for digital evidence.

To some extent, the MLAT process has always been challenging. A request for information must be carefully crafted and passed through multiple intermediaries to the foreign partner responsible for gathering the evidence. At many of the points in this process, an intermediary is responsible for carefully aligning the request for compliance with the needs of the host and the requesting countries; assessing such potential legal conflicts, inconsistencies, or inadequacies as insufficient civil liberties protections; and ensuring that the request meets evidentiary standards for provision of the evidence from the host country (Access, 2017b). Therefore, there are some irreducible complexities and time-consuming elements in the process, and, until recently, there was comparatively little concern over the known issues. However, the proliferation of cloud computing and remotely stored data, especially by transnational organizations in an increasingly globalized world, has caused a dramatic increase in the need for MLATs for extraterritorial digital evidence. For example, the number of MLAT requests to the Criminal Division of the Office of International Affairs (OIA) increased by 60 percent overall from 2005 to 2015, and a significant proportion of this increase was the result of a tenfold increase in requests for electronic records (U.S. Department of Justice, 2014).

The time-consuming nature of the process has been cited as a major roadblock as the number of requests has grown. Even when the process might otherwise go quickly, the authority to compel record disclosure rests on national statutes governing electronic records, and the uncertainty and ambiguity in the statutes present challenges in the MLAT process. Furthermore,

the overall process significantly lacks transparency. Individuals interested in the outcome of a request frequently have no way to obtain information on its status or the interactions taking place while the request is making its way through the process. Finally, there are gaps in the MLAT system: There are multiple countries that the United States has no treaty with. As a result, it may be difficult or impossible to adequately exchange evidence with these countries (Access, 2017a). The challenges and problems with the MLAT system can often lead to the impression that using the MLAT process is, at best, a waste of time and, at worst, an insurmountable barrier to acquiring the needed evidence through legitimate legal means (Woods, 2015).

The unduly burdensome MLAT process presents a challenge to international comity insofar as it provides a perceived rationale for extraterritorial application of national laws both within the United States and without.⁶ In addition to the specter of conflicting international legal obligations on providers, such extraterritorial application or the perceived threat thereof has led to the rise of data localization mandates. As the United States retains a kind of “home-field advantage” with many U.S.-based service providers, foreign nations have become concerned with the access the United States might have to data stored in their territories by legal means circumventing an MLAT request, especially where that access may conflict with their laws or privacy rules. The result has been a push to mandate that data be physically located in their territories, and thus in their control. The problems associated with data localization mandates have been thoroughly explained elsewhere (Chander and Le, 2014), and proposed reforms of the MLAT process have been intended as means of mitigating the rise of such mandates (Daskal and Woods, 2015).

The Relationship Between Law Enforcement and Service Providers

Service providers have publicly shown concern over the trend toward data localization and a system that is inadequate to handle an increasing number of extraterritorial data requests (Microsoft Corporation, 2014). Even situations that do not involve extraterritorial data requests, however, are frequently fraught with challenges for both law enforcement and service providers. The preceding section detailed the ways in which service providers must be relied upon by law enforcement in

the acquisition of remotely held digital evidence and how their perspectives on the process and their priorities may not always align closely with those of law enforcement. This misalignment can lead to a situation where the relationship between the two tends to be adversarial as each pursues differing priorities.

The scale of involvement service providers must now have in the process is one source of growing strain, as the number of data requests from law enforcement has grown over time. The annual transparency reports published by many of the larger providers quantify the burden placed on providers to fulfill these requests. In just one provider example, Google’s transparency report noted that it received over 90,000 data requests internationally in 2016 and provided data in more than 60 percent of cases. In the United States alone, over 27,000 data requests were made, and nearly 80 percent, or about 22,000 instances, resulted in the provision of data. Furthermore, the number of data requests has significantly increased nearly every year since the data were first published in 2010 (Google Inc., 2017).

Providers can also be subject to requests from law enforcement that are difficult to understand or comply with because of law enforcement’s inexperience or ignorance of their proprietary service architecture. Because of the complicated way providers may use or store data, compliance is likely to involve much more than the simple transfer of files or hard drives or the reconstruction of certain user files. As such, some data requests from investigators who are unaware of the provider’s architecture may be technically impossible or infeasible to comply with. For example, an investigator may request activity logs for a user as part of a forensic investigation. However, if the service provider’s architecture does not regularly synchronize users’ virtual machines with a persistent storage, the data and activity logs being requested might have been lost and become unrecoverable when the suspect shuts down his or her virtual machine. Although the investigator has made a reasonable request for activity logs, the service provider may not have the technical capability to comply. Furthermore, service providers may be unclear on the appropriate standard or legal process the government uses to compel access to customer data. Providers may not have clear guidance on how to appropriately respond to, for example, requests that come from other states, requests

⁶ See, for example, Brazil’s law attempting something similar: Hogan Lovells, undated.

The nature of the relationship between law enforcement and service providers may have an inherent tendency toward becoming adversarial rather than cooperative.

that require broad collection of customer data,⁷ or requests for certain data types with legal instruments possessing lower evidentiary burdens (i.e., a subpoena versus a warrant).

The murky legal authority granted by the statutes with respect to current technology may put providers in a challenging position. In the past five years, companies have seen economic disincentives and competitive disadvantage from being viewed as overly permissive or cooperative with government data requests, especially when these requests are insufficiently particular. Technology companies have been publicly criticized for too willingly participating in overly broad data-collection efforts. Since revelations of government surveillance efforts in 2012, they have been publicly competing with one another and have been graded on their commitment to protect user data from government requests so as not to be seen as “selling out” their users relative to their competitors (Wyatt and Miller, 2013).

At the same time, law enforcement agencies have voiced frustration over what they perceive to be the capriciousness and obstruction of providers when served legitimate requests based on firm legal authority and justified needs for criminal investigations. In a report published in 2015, the International Association of Chiefs of Police (IACP) lamented that providers were increasingly reluctant to comply with legitimate law enforcement requests. Nontechnical barriers are also encountered by law enforcement when issuing requests, including

- erratic intake of court orders and subpoenas
- delayed or unpredictable responses
- inaccurate, incomprehensible, or imprecise responses
- prohibitively expensive responses (IACP, 2015).

One workshop participant provided a specific example of this phenomenon. When officers would issue search warrants for the data from very active users of one of the major social

⁷ *Broad collection* encompasses both (1) collection of many different users’ data and (2) collection of a wide range of data for a single user over a long period. Both types of data collection have faced legal objections from privacy advocates.

media platforms, the social media provider would provide data in the form of a single PDF file, or HTML file if requested. The files provided were described as unreadable by the receiving officers. They were frequently so large that they would crash the programs or browsers to which the officers had access. Furthermore, the data contained in the files were scattered without a recognizable order or easy way to search for relevant information. While a software tool had been developed to parse previous data formats, law enforcement had no tools for this format. One officer noted that not only would the provider refuse to provide tools to help officers parse the data, but also that the purchase or organizational development of tools was seen as a risky endeavor, because providers change formats often, and the tool would shortly become useless. One officer described being treated like a nuisance by a provider’s compliance personnel. While the provider technically complied with the order to provide the data, backed by a legitimate search warrant and investigational need, the response presented a serious obstruction to law enforcement investigations.

In addition to such practices, where data are technically provided but in a format that may hinder their use in the investigation, the provider may in some cases refuse to comply with the request at all. Data provided by some of the major technology companies for 2016 indicate that between 66 percent and 81 percent of government data requests resulted in the provision of some data (Wong, 2016). Thus, between 19 percent and 34 percent of the time, the company refused to comply with a government data request. While providers may have reason to refuse compliance in some cases, the heavy reliance that law enforcement must have on service providers to obtain evidence in investigations makes refusal in the case of disagreement over the request a serious challenge.

The nature of the relationship between law enforcement and service providers—where law enforcement must rely heavily on service providers, and providers may be compelled by law to respond to requests that are at least moderately burdensome—may have an inherent tendency toward becoming adversarial rather than cooperative. Surveys show that the public is increasingly concerned with how corporations handle

their data (Microsoft Corporation, 2013; Rainie and Duggan, 2015) and that these corporations see a concomitant competitive advantage in publicly boosting their ethical data practices (Accenture, 2016). The challenge then arises when even routine cooperation with law enforcement data requests may be perceived by some as “selling out” users, and obstruction is included in the push for competitive advantage. In this case, the laudable push for better corporate data ethics may unintentionally result in, at best, increased obstruction for regular lawful investigative activity and, at worst, a growing animosity and adversarial relationship between law enforcement and service providers. In the long term, this problem may only be solved by shifting incentives toward cooperation by gradually improving the publicly perceived legitimacy of law enforcement actions that has diminished in the wake of recent revelations of broad government data-collection efforts.⁸ In the interim, however, solutions are needed that will improve the relationship and cooperation between law enforcement and service providers and improve data requests, which will mitigate the burdens on both.

Reform Proposals

As a result of the inadequacies of the status quo, multiple proposals for reform have arisen. These proposals seek to remove the ambiguous legal standards discussed earlier and to bring law into accord with modern electronic communication technology, especially with regard to the internet, mobile devices, and cloud computing and storage that were either nascent or nonexistent at the time of the ECPA’s passage. Many of the same proposals recognize the problems with the current MLAT system and also attempt to reform portions of that system.

A consortium of organizations called the Digital Due Process Coalition—composed of digital privacy advocates, purveyors of digital information, and providers of electronic communications and storage services—has proposed a series of changes to existing law as a starting point for reform. These proposed changes would first require a warrant for disclosure of location information, whether in real time or retrospective, as location information is currently viewed as noncontent information that requires only a subpoena for access. They would further eliminate distinctions for communications based on duration of storage, means or status of storage, or provider type and would make a uniform standard for all other noncontent

information, such as metadata, that would require a court order for access. Finally, for the remainder of data that require only a subpoena for access, the changes would require greater particularity in subpoena power, such that it must be limited to a single account or individual per subpoena, with any broader request requiring a court order. Cumulatively, these changes would create uniform standards that eliminate many of the ambiguities, including those associated with the definition of electronic storage or the distinction between ECS and RCS providers (Digital Due Process Coalition, 2017). Others echo some of these proposals, including the establishment of a single standard for access to all content data held by or for a user (Kerr, 2014).

Several guiding principles have also been suggested to guide any MLAT reform efforts. Any reform efforts must accommodate and enable justified and proportional access for legitimate authorities; human rights protections; and better transparency, efficiency, and scalability for the process. Specific improvements would make an MLAT request electronic and easily tracked, institute uniform request formats for requesting countries, and provide adequate staffing and time limits for responding to requests. Furthermore, a consistent and public corporate policy for responding to requests (especially in countries where no MLAT exists) could reduce frustrations among law enforcement personnel over perceived capriciousness or obstruction in service provider responses (Woods, 2015).

Since 2011, various items of legislation have been introduced to the U.S. Congress to implement changes. The ECPA Amendments Act of 2011, the Email Privacy Act, and the Online Communication and Geolocation Act were all introduced in the 113th and the 114th Congresses, but were never enacted. Each of these acts contained similar provisions. The amendments would have specifically added geolocation information services as a protected record category that providers would only be compelled to disclose with a warrant and would have removed the standard based on duration of data storage, among other minor changes (U.S. House of Representatives, 2015b). The Email Privacy Act has also been introduced in the 115th Congress and has been referred to the Senate Judiciary Committee (U.S. House of Representatives, 2017).

Proposals have also been made and legislation introduced to better deal with issues of data and evidence territoriality. This issue includes not only the jurisdictional authority implied in U.S. law, but also the ability of service providers to voluntarily provide data to foreign governments, the metric used for establishing territoriality, and the challenges associated

⁸ For commentary, see, Jackson, 2015.

with using the MLA process. The Law Enforcement Access to Data Stored Abroad (LEADS) Act was introduced in the 114th Congress and aimed to remedy some of these issues. It would have included a provision granting government authority to obtain with a warrant any content records belonging to “U.S. persons” (citizens or lawful permanent residents) stored, held, or maintained by a provider. The act also would have included reforms to the MLA process intended to better track and expedite the process, including the creation of a publicly available MLAT request form and an online docketing system for requests. It further would have required that data on the number of incoming and outgoing MLAT requests and the time taken to fulfill them be published online, that preservation orders may be issued upon receipt of an MLAT request, and that providers must be informed in writing when a data request is made pursuant to an MLAT (U.S. Senate, 2015). The LEADS Act was replaced by the International Communications Privacy Act (ICPA), introduced by Senators Orrin Hatch of Utah, Christopher Coons of Delaware, and Dean Heller of California in 2016, with an identical version in the U.S. House of Representatives. The ICPA, if passed, would also create a legal framework requiring law enforcement agencies to obtain a warrant for all content, authorizing law enforcement to obtain communications of U.S. persons regardless of location, and making reforms to the MLAT system (U.S. Senate, 2016).

While these reform proposals would be promising steps if implemented, the issues they intend to fix remain problematic in the interim. While these problems remain, such counterproductive solutions as data localization mandates may continue, to the dismay of service providers, advocates of civil liberties and an open global internet, and other stakeholders alike. Furthermore, even if these reforms are successful, challenges will remain that are not tied to legislative fixes. An adversarial relationship stemming from differing perspectives and priorities for service providers and law enforcement will continue to be problematic for both, and poor relationships between some countries will continue to frustrate mutually beneficial data-sharing even if many of the MLAT reforms are implemented. Digital evidence held in remote data centers, therefore, is associated with a number of both technical and nontechnical challenges that should not be left merely to potential legislative fixes. The preceding sections discussed the relevant background information and various issues. The following sections describe the workshop, which brought together a diverse group of experts on the topic to discuss the challenges with digital evidence held in remote data centers to identify and prioritize research needs.

WORKSHOP ON CHALLENGES WITH DIGITAL EVIDENCE HELD IN REMOTE DATA CENTERS

In May 2017, the RAND Corporation and the Police Executive Research Forum held a workshop in Washington, D.C. Similar to our previous workshop examining issues with digital evidence more generally, this workshop was intended to go beyond merely identifying needs on a subject to find potential solutions and elicit expert prioritization of those solutions. The goal of the workshop was to bring together a diverse group of experts and practitioners to discuss issues related to digital evidence held in remote data centers for the purpose of identifying both problems and potential solutions. We provide a general description of the preparation for the workshop, including selection of the participants, scope, specific topics for discussion, and a thorough description of the workshop discussions.

Preparation for the Workshop

The subject of the workshop was selected based on informal discussions with participants from the previous digital evidence workshop and a literature review. Previous participants were asked for input on what digital evidence issues endured for them since the previous workshop and what new issues may have arisen. In these discussions, multiple concerns were raised over access to and retrieval of digital evidence held with remote third parties. A literature review was performed to identify the scope of a workshop on this subject. A preliminary list of challenges was created from this review, which was used to identify potential participants, who were then invited to attend the workshop. The list included issues associated with

- ambiguity in authority granted by U.S. law and inconsistent privacy protections
- extraterritorial evidence and the MLAT process
- data localization mandates
- coordination with service providers
- technical challenges associated with evidence held in the cloud.

Seventeen panel participants ultimately accepted the invitation and attended the workshop. This included seven law enforcement personnel, one prosecuting attorney, two lawyers, three professors, two individuals in the private sector, one privacy advocate, and one laboratory researcher. Six project staff

Workshop Participants

Jennifer Daskal

American University Washington College of Law

Josiah Dykstra

Laboratory for Telecommunication Sciences

Edward German

Macon County, Ill., Sheriff's Office

Paul Kammerer

Volusia County, Fla., Sheriff's Office

Timothy Laham

Boston, Mass., Police Department

Sean M. Larson

Hathaway & Kunz, P. C.

Troy Lawrence

Fort Worth, Tex., Police Department

Erik Laykin

Duff and Phelps, LLC

Jeff Matthews

Arlington, Tex., Police Department

Mark MacCarthy

Software & Information Industry Association

Joseph J. Schwerha

California University of Pennsylvania

Joseph Spataro

Florida Attorney General's Office

Derreck Spencer

Salt Lake, Utah, FBI Cyber Task Force

Lee Tien

Electronic Frontier Foundation

John Randy Tyler

Perkins Coie, LLP

Andrew K. Woods

University of Kentucky College of Law

Michael Yu

Montgomery County, Md., Police Department

and five officials with the U.S. Department of Justice (DOJ) also attended.

Approximately two weeks before the workshop, a read-ahead for the participants was prepared based on the literature review of the identified challenges. The read-ahead and a pre-workshop questionnaire querying participants on their particular concerns was sent to confirmed attendees. The questionnaire first asked attendees to rank matters of law and procedure according to their perception of the various matters' importance and degree of difficulty as obstacles to investigatory efficiency, then asked them to do the same for technical matters. Next, participants were given the opportunity to comment on problems, challenges, and opportunities they saw in each of the issue categories and identify any important issues that may have been missed in the read-ahead and pre-workshop questionnaire. The responses from participants were collected and used to narrow the scope further and provide a starting set of discussion topics for the workshop.

Workshop Discussion

The workshop began with a brief introduction, including a discussion of the results and priorities gleaned from the pre-workshop questionnaire. For each of the subjects under discussion, participants were asked to consider the issue with the objective of identifying any problems, opportunities, or needs in three categories: law enforcement investigation effectiveness, privacy issues, and needs and incentives for service providers and their customer base. The discussion was focused on two areas—(1) policy, process, and procedure and (2) technical issues—with the majority of the discussion dedicated to the first area. As the discussion proceeded, the moderator would occasionally call participants' attention back to the generation of a specific need that could be distilled from the opinions being expressed and add it to the list of needs for later refinement and prioritization. In this section, we summarize the workshop discussion that generated the list of needs, beginning with the issues connected to U.S. law and procedure.

Policy, Process, and Procedure U.S. Law and Procedure

One participant made the observation early in the discussion surrounding U.S. law and procedure that there is no unambiguous and viable legal authority for obtaining remote digital evidence for the vast majority of law enforcement, and this

problem extends even to the level of requesting data from a U.S. provider in another U.S. state. Another participant bluntly commented in the pre-workshop questionnaire that “jurisdiction can be a confusing mess.” Indeed, participants were in agreement on the uncertainty and difficulty surrounding obtaining digital evidence held in another state. It was noted that the degree of difficulty depends, in part, on whether or not the state has a “long arm” statute,⁹ but challenges remained regardless. Discussion on this topic focused on the interrelated issues of confusion around establishing proper jurisdiction and authority for search and seizure, the appropriate legal process to follow for the particular evidence required (e.g., subpoena, court order, or warrant), insufficient training or access to knowledge or procedure, and the need for better interagency coordination and cooperation. One law enforcement participant also asserted that officers “want to know the process and will follow it, but they need to know that it will work when they do.”¹⁰

Law enforcement participants noted that officers often lack the necessary information or training to navigate the legal process effectively because of the confusing legal language and uncertainty around jurisdiction. State accreditation standards for law enforcement may or may not include basic familiarity with digital evidence requests. Furthermore, participants noted that local judges often also are uncertain about their authority to issue a search warrant for evidence outside their jurisdiction, and law enforcement officials then need to approach them to explain that authority.¹¹ In some cases, local state agencies may approach federal courts to obtain warrants, but participants observed that this can be difficult. As such, law enforcement officers and prosecuting attorneys must be sure that particular courts have the jurisdiction to issue the needed search warrants. Participants suggested that a system or tool that helped officers craft warrants compliant with the appropriate jurisdiction could be helpful. In later comments, however, it was noted that

this would not ultimately eliminate the legal ambiguity about jurisdiction, and a legislative solution may be required.

Law enforcement participants noted that some of these challenges could be mitigated with better communication and collaboration with investigators from other agencies with experience in making similar requests. While it was noted that online email list servers can be a useful resource, it was also pointed out that many portals and list servers already exist but are not well known among investigators. At the same time, participants brought up the idea that such tools for collaboration and communication would be less necessary if there were a useful standardized procedure for requests that was available and widely known. Multiple law enforcement participants spoke of the usefulness of the site Search.org in providing a wealth of helpful information, and it was suggested that such a site could be incentivized to become a platform for information like this.

There was also discussion around the idea that the lack of clarity in the law may sometimes lead to an unstated assumption that all extant data relevant to an investigation should somehow be made available to law enforcement. From this perspective, the default view is that barriers to law enforcement access are unnecessary burdens or hurdles to be overcome, rather than potential safeguards of citizen privacy. In addition, in this view, providers often might not be seen primarily as businesses for whom compliance with a third party’s demands is a significant burden, but rather as holders of evidence. One participant commented that “cloud service providers are not simply repositories of digital evidence to be used in law enforcement investigations,” and the potential that they are viewed as such may be a barrier to effective cooperation. Needs related to U.S. law and procedure are summarized in Table 2. Many of the concerns voiced over U.S. law and procedure overlapped significantly with discussion on law enforcement and service provider cooperation and coordination. These elements of the workshop discussion will be summarized next.

Service Provider Coordination

A significant portion of the discussion at the workshop was related to challenges with service provider and law enforcement coordination. Participants discussed issues that were concerning from both the provider and law enforcement perspectives, as well as from the perspective of customers whose data privacy may be affected by their interaction. Participants noted that new platforms, which may eventually hold evidence of value to

⁹ A *long-arm statute* is a law that gives a court personal jurisdiction over a nonresident defendant if certain conditions are met. For more detail, see Vedder, Price, Kaufman, and Kammholz, P.C., 2003.

¹⁰ We emphasize that participants’ views expressed in this report should not be construed as being for or against obtaining warrants for various evidence; rather, they are focused on facilitating access to evidence, assuming that the government obtains adequate legal authorization.

¹¹ FRCrP 41 does allow warrants to be issued for remote access to data in another jurisdiction, although only in limited circumstances.

Table 2. Identified Needs Related to U.S. Law and Procedure

Problem or Opportunity	Associated Needs
There is no database for contact information for specialists who deal with remote digital evidence.	<ul style="list-style-type: none"> • Create a database or portal where law enforcement can access contact information, documentation, and training for accessing remote digital evidence.
Investigators are often unaware of the kinds of information that can be requested and the options for bounding their requests.	<ul style="list-style-type: none"> • Develop standardized online training for investigators to assist with requesting evidence and data. • Develop an online repository (i.e., a clearinghouse) for best practices in making digital evidence requests.
Procedures for serving legal process are often not well-defined or are unclear.	<ul style="list-style-type: none"> • Develop standards that are easier for providers and investigators to comply with.
It can be difficult for an agency in one state to obtain a warrant to get data from a provider in another state—judges often do not feel they have the authority.	<ul style="list-style-type: none"> • Conduct research on model statutes that could improve the procedures for serving and responding to legal process. • Develop a Turbo Tax–like system for preparing warrants that are compliant with the appropriate jurisdiction.
It is often difficult to determine which jurisdiction has the authority to compel production of the data and, thus, where the legal process or MLAT should be served.	<ul style="list-style-type: none"> • Facilitate the development of a uniform system of jurisdiction over data in the cloud.
Search warrant parameters imposed by judges are often not aligned with the technical limitations of the systems and devices being searched.	<ul style="list-style-type: none"> • Develop an information exchange system where investigators can share information on points of contact and best practices for search warrant “design.”
Blocks of IP addresses are often reassigned or subleased to other providers, making it difficult to identify the actual internet service provider (ISP) with the customer relationship.	<ul style="list-style-type: none"> • Conduct research and analysis to highlight the impact on law enforcement with regard to ECPA’s prohibition of voluntary disclosure of customer communications records to governmental entities (U.S.C. 2702(a)(3)).
A large number of cybercrimes cannot effectively be investigated using local resources (e.g., ransomware attacks).	<ul style="list-style-type: none"> • Evaluate the efficacy of specialized task forces focused on lower-level cybercrimes. • Develop a standard set of vetted resources (e.g., nomoreransom.org) that can be shared via agency websites.
There are few published “how-to” procedures that practitioners can follow to request data from data custodians (i.e., providers). Thus, the learning curve can be very steep for investigators who are not familiar with current processes.	<ul style="list-style-type: none"> • Develop a “50-state guide” on search warrant procedures (if it does not already exist).
Even when investigators follow the appropriate processes, they may still have difficulty obtaining the data that they requested and have the authority to obtain.	<ul style="list-style-type: none"> • Conduct research to assess the risks and benefits of domestic and international sanction regimes.
It is difficult to make contact with experienced investigators from other agencies who have recent or relevant experience with requesting data or evidence.	<ul style="list-style-type: none"> • Suggest that the professional organizations (e.g., state attorneys general, IACP) collectively examine the issue and produce templates for search warrants.
The methodologies for acquiring evidence are constantly evolving.	<ul style="list-style-type: none"> • Develop model statutes for federal, state, and local legislatures that are often updated to address the current state of technology.

police investigations, develop very quickly, and that these platforms and providers are often resistant to police partnerships.

Furthermore, participants discussed their perception that most of the difficulty in obtaining evidence arises because providers are the presumed gatekeepers of user data in the eyes of their customers. It was noted that, if law enforcement requested a business record that was the property of the service provider, the process was much simpler and easier. Participants expressed a desire for the modernization and standardization of privacy law and procedures and suggested legislative solutions to some of the problems. One participant spoke optimistically about legislation like the ICPA, which was introduced by Senators Hatch, Coons, and Heller (U.S. Senate, 2016), while another expressed concern with this particular approach. That being said, most of the discussion focused on nonlegislative solutions for better cooperation and understanding.

Law enforcement participants frequently voiced the need to find “a human to talk to” when they needed to interact with service providers. In addition to the need to know where to serve legal process and with whom to speak about it, investigators would like to be able to find a representative with whom to discuss specific needs and preferences in the data request, but they frequently lacked the ability to find a suitable point of contact. Participants expressed the desire for published guidelines on data requests from providers and a list of points of contact for law enforcement. They acknowledged that the new, small providers that arise year after year would inevitably lack these things. Participants provided several examples of useful resources, including the FBI Operational Technology Division, U.S. Department of Homeland Security Cybersecurity Division, DOJ Computer Crime and Intellectual Property Section, and Search.org. Additionally, the FBI Law Enforcement Enterprise Portal was mentioned as a useful resource populated with helpful training and tools for law enforcement, as well as a means for securely transferring digital evidence. Sprint’s L-site, a system that gives law enforcement an online portal to submit, track, and receive responses from the company, was mentioned specifically as a good example of a system that functions well for facilitating law enforcement and provider cooperation.

Related to issues with finding appropriate provider personnel to contact and to serve legal process to, law enforcement participants voiced exasperation over provider responses to their requests. These participants frequently noted the desire to be “able to obtain all the evidence from the provider, in its entirety and in a timely manner,” and preferably as a reconstruction of the files in the suspect’s account as the user would have seen

Law enforcement participants frequently voiced the need to find “a human to talk to” when they needed to interact with service providers.

them. Instead, it was observed that officers were often met with delaying tactics; data formats that were frequently changing and often made law enforcement analysis intractable; and, occasionally, with outright refusals to comply or with no response at all. One participant opined that the biggest problem was getting a data center to comply with an out-of-state warrant. The participant stated that providers often fail to recognize search warrants from other states and try to require that the warrant come from an agency that is local to them.

Another participant suggested that some providers may intentionally obfuscate the data to make it harder to read. While acknowledging that companies may frequently change their data formats internally, this participant noted that some types of data and their metadata do not change frequently, such as emails or word processor documents, and they saw no reason that these could not be provided in a consistent, analytically tractable format. Even something as simple as the provision of a cover sheet with parsing instructions for the data set was suggested as a solution. One participant acknowledged that providers are often viewed as the gatekeepers of customers’ data and that providers thus might see little incentive to streamline their responses or make them more convenient for law enforcement as a way to be perceived as further protecting their customers’ data. The participant then noted that, despite this, the “inefficiencies built in[to] the process should not be the primary way of defending citizens’ civil rights.”

Other participants noted the converse of some of these observations, commenting on the burden the requests can put on the provider, especially when the request from law enforcement is poorly worded, ambiguous, technically infeasible, or impossible to comply with. Companies design their data structures in a manner that is most advantageous and efficient

for their primary business purpose, not with the priority of making the resulting data analytically tractable for law enforcement. Participants also cited the often hundreds, thousands, or tens of thousands of such requests some companies must fulfill each year, noting that this is already a substantial burden that is peripheral to their business activities. As such, the amount of additional work that would be required to reformat data to individually fit law enforcement requests may be viewed as costly, unnecessary, and, most importantly, not legally obligatory. One participant later commented that there is no existing legal obligation to provide data in a specific format, and companies may resist the imposition of such an obligation. Some providers may attempt some small aid in interpretation if they understand the issue, but boilerplate requests from law enforcement for this might be ignored. This can often lead a provider to perform the minimum that is legally required, sometimes leaving the investigator with data that technically meet the terms of the request but are not ultimately very useful. Participants also discussed the merits of offering financial incentives to comply with government requests as a way of offsetting the costs of compliance. This suggestion had mixed reactions from the participants. One participant later flatly commented, “there should not be financial incentives for complying with a court order.” Another noted that providers can already seek reimbursement for compliance, but many do not because of public pressure, so it could be unlikely that providers would alter their business model and better comply with requests to obtain these incentives. This participant thought that financial incentives may instead have a different effect: Rather than directly improving the quality and speed of compliance, having providers quantify the costs and burdens involved in complying with requests may lead to a greater understanding of the challenges of compliance. This could alter perspectives for stakeholders, allowing better communication and possibly indirectly improving compliance with requests.

Similar to investigators’ challenges in working with the data sets they receive from providers, participants also discussed how the format of the request from law enforcement or the kind of data that is requested can be hard for provider representatives to understand. This is exacerbated by a related issue brought up by many participants: Provider networks and structures are opaque to law enforcement from the outside, and even when officers have visibility into the systems, they may not have sufficient training to understand the information. This will leave the officer without the knowledge to craft a better request and often leads to misalignment between how data

are requested and how they are stored. This extends to search warrant parameters imposed by judges that are not aligned with the technical limitations of systems or devices holding the data. Better industry cooperation was suggested as a potential solution to address this, although others suggested that proprietary information and an adversarial relationship between law enforcement and providers may be roadblocks. Participants discussed the potential benefit from some sort of precoordination between law enforcement and larger service providers as a means of improving communication and avoiding the risk of “surprising” the provider with a request. This was likened to the “conferral” step in civil cases, which allows two-way communication between requesters and providers. One participant noted that law enforcement guidelines are supposed to cover these things, but they often cannot keep up, and standardized training for law enforcement requests was floated as a possible solution. Furthermore, it was noted that if investigators are planning on requesting a gag or preservation order, they can still contact providers to have a discussion in the abstract about the best ways to construct the request so as to facilitate better outcomes for both.

Participants also noted that it can be difficult or impossible to verify the trustworthiness of data supplied by the provider, especially given the observed lack of sufficient communication or coordination. One participant asserted that “there is no way to guarantee the trustworthiness of data preserved and delivered by a service provider.” Another stated the problem as, “authorities don’t know what they don’t know,” and they have no way to ensure the completeness of produced data. This includes issues with completeness, lack of tampering, and production of evidence with proper attribution. It was noted that, traditionally, criminal investigators have collected their own information, while civil cases relied on discovery, where the other party was trusted to produce the right information. However, participants observed that more trust is now required in criminal cases because providers are producing the data. Finally, the issues of customer notification, data retention, and evidence-preservation orders were discussed. Participants lamented the detriment to investigations when suspects were tipped off to destroy evidence by provider notifications, particularly in child exploitation cases. Lack of data retention was also noted as a problem, especially when the request was made of foreign entities, which are sometimes required by law to destroy data after a certain period. Needs related to service provider coordination are included in Table 3. Participants noted that preserving evidence in its entirety while investigators

Table 3. Needs Related to Service Provider Coordination

Problem or Opportunity	Associated Needs
Finding the contact information and communicating with providers' legal representatives can be extremely difficult.	<ul style="list-style-type: none"> • Develop an information exchange system where investigators can share information on points of contact and the types of data available via different providers.
There can be a misalignment between the way that data are requested and the way that they are stored. Without sufficient communication between the requestor and the provider, the result can be unhelpful.	<ul style="list-style-type: none"> • Conduct research and interviews on what service providers are willing to do to facilitate the exchange of information that should legitimately be provided in response to legal process.
The requests made by law enforcement are often difficult or impossible for data custodians (i.e., providers) to comply with.	<ul style="list-style-type: none"> • Develop curricula and training materials that help law enforcement trainers construct requests that are more technically feasible. (Curricula and training materials are potentially reviewed by provider industry groups.)
Data custodian procedures frequently change, which often frustrates the ability of law enforcement to reuse previously successful procedures.	<ul style="list-style-type: none"> • Develop a "standard" for law enforcement requests to industry for user data.
There is a lack of financial incentives for service providers when attempting to comply with legal process inquiries.	<ul style="list-style-type: none"> • Catalog the difficulties that the service providers experience when attempting to comply with legal process.
There are no standards for data retention.	<ul style="list-style-type: none"> • Develop a catalog of existing industry practices (as a means of informing investigators and potentially suggest a common guideline or standard).
Provider data formats are often not machine-readable and tools are not provided to read them.	<ul style="list-style-type: none"> • Develop best practice boilerplate language for requesting data. For example, data should be in a native format or file; be machine-readable; and, if the format is proprietary, a reader or decoder should be supplied.
It is still difficult to know where to serve legal process to obtain user data inside the United States.	<ul style="list-style-type: none"> • Develop a guide to educate providers and device manufacturers on how law enforcement prefers to request data and interact.
There is a lack of clarity on provider interpretation of jurisdiction over their legal organizational architecture and choices they have made to ensure data residency and jurisdiction.	<ul style="list-style-type: none"> • Conduct research and analysis on provider information technology or organizational architecture and the implications for U.S. and foreign jurisdiction.

wait for an MLAT request, for example, was a particular issue. MLATs, extraterritorial evidence, and procedures and issues around data requests to and from foreign entities are discussed in the next section.

Extraterritorial Evidence and MLATs

Discussion around extraterritorial evidence focused on the notion espoused by one participant that "data [go] everywhere, but laws are territorially focused." Furthermore, investigations by state and local law enforcement are a local matter, but cyber investigations, cybercrime, and crimes primarily involving digital evidence can easily span the globe, and many such crimes cannot be investigated purely with local resources. Participants noted that local agencies often have a difficult time managing the changing environment with annual budget seasons and

limited resources. While some participants suggested the infeasibility of solving much of this crime without relying on federal assistance, discussion shifted to the success of regional task forces as an alternative. Participants noted that such regional task forces have shown that they could manage the problem without much need for federal assistance, and the institution of task forces for network crime and cybercrime in each state would be very beneficial. Nevertheless, participants observed that even specialized task forces need to have a threshold of crime severity on which to focus their limited resources.

The use of the MLAT by practitioners at the state and local level was also a prominent part of the workshop discussion. Participants had mixed reactions in discussions around the use of MLATs at the state and local level: One participant suggested that it would not be feasible for the local level to ever use an MLAT, while another stated that his or her interaction with

Cyber investigations, cybercrime, and crimes primarily involving digital evidence can easily span the globe. Many such crimes cannot be investigated purely with local resources.

the MLAT was as “straightforward as [I] expected,” but was time consuming. Many participants echoed this idea, saying either that the use of the MLAT process was straightforward but was too time consuming or that the process was too opaque and was too inefficient for law enforcement needs overall.

Indeed, one participant noted that merely the mention of MLAT in the context of an investigation would discourage him or her from proceeding. In discussions around the lengthiness of the process, one participant noted that “six to nine months for the process makes regular, proper investigations impossible.” The Microsoft decision was brought up in this context as well (*Microsoft Corp. v United States*, 2016), reflecting the idea from the U.S. law and procedure discussion that law enforcement wants to know the process and follow it, but it needs to know the process will work. Participants suggested that, when the proper process creates an impassable roadblock to a legitimate investigation, people inevitably will try to find alternative means with murkier legal authority to avoid it.

While participants discussed the current inefficiencies and insufficiencies of the system, they also noted that some hurdles in the process will always be present, such as language barriers and that, to some degree, the process is supposed to be slow and methodical. Some participants suggested that this complicated legal process should be fairly difficult: The process needs a neutral, detached magistrate to focus on the lawfulness of the request, and it needs to be vetted at several different levels. Legal paradigms may be significantly different between two countries, and the request will require careful scrutiny for compliance with both. For example, such U.S. legal principles as the notion of probable cause can confound foreign counterparts. Additionally, if the requests are “bad” or overbroad, the process is *supposed* to be very difficult. Despite this, there was general agreement that the process was much too inefficient for current needs, and participants discussed various elements of reform.

Despite significant literature and public discussion on the subject, one participant suggested that “we have not yet tried

to really improve the MLAT process. More resources need to be put into it.” The first step toward this, the participant stated, is to do the research to find out what the bottlenecks in the process are. To act on reform, we need to better understand what about the process is actually in need of reform—instead of observations that the process takes too long, we need to determine the steps that are particularly time consuming and what can be done to increase efficiency. A participant later suggested potential options: “Is it review within the U.S. government? DOJ? [U.S. Department of] State? Or is it the process within the courts? Could you increase personnel in the courts? More magistrate judges? More clerks for existing magistrate judges?” Other suggested possible bottlenecks include insufficient training of foreign or domestic staff and insufficient staff in the offices that handle MLAT requests.

Participants offered and discussed many avenues to improve the process. The opacity of the process was a particular frustration for law enforcement, and an online docketing system that would allow investigators to submit requests and track their status and progress through the system was suggested as a helpful improvement. Participants mentioned that the DOJ OIA is preparing an online docketing and tracking platform, but it is currently held up by inadequate funding. This idea was also part of the ICPA proposed by Senators Hatch, Coons, and Heller and was agreed to be beneficial in improving the accessibility and transparency of the system (U.S. Senate, 2016). Legislation like the ICPA was discussed as a potential solution to some of the issues, but the discussion largely focused on non-legislative means of solving issues. Another avenue for improvement is the creation of better or more-accessible guides for law enforcement when making MLAT requests. One participant noted that the website MLAT.info has valuable information but is not always up to date. Similarly, participants noted that there is no worldwide set of guidelines for the process; needs vary by location, type of service, and legal process. In this context, some participants discussed the potential benefits of an organization like Search.org (which provides many helpful

law enforcement and compliance guides for domestic requests), which could focus on international requests. Related to the variability from country to country, the gaps in the MLAT system were also discussed. Participants acknowledged that a critical step in MLAT reform will need to be establishing agreements of some kind with countries that currently have no MLAT because data in these countries are currently viewed as inaccessible to law enforcement. Needs related to extraterritorial evidence and the MLAT process are summarized in Table 4.

Technical Issues

The last portion of the workshop discussion was directed toward technical issues law enforcement faces with respect to remote digital evidence. Technical issues similar to those discussed in the previous digital evidence workshop made an appearance, including issues related to the cost and volume of stored data, especially when attempting to transfer or acquire them remotely. The technical issue discussion began, however, with evidence access issues for remote government databases. Participants noted that law enforcement consistently lacks access and connectivity to other U.S. federal repositories of digital evidence, including databases for latent fingerprints and facial recognition.

The FBI maintains the databases for latent prints and mugshots that law enforcement agencies can probe, and the mugshot repository allows automated facial recognition searches for authorized law enforcement agencies. These agencies can submit a photo to be searched against the repository, and they receive candidate photos that they may manually

match to a suspect as an investigative lead (although not as a positive identification) (Del Greco, 2017). The lack of access to these repositories was attributed, in most cases, to a lack of funding for the workstations that would enable state and local law enforcement to connect to the FBI databases, as well as for training personnel to use the workstations. Participants also discussed the matching accuracy for latent fingerprints in the latent prints database. The transparency and accuracy of the matching algorithms was unknown to the participants, and it was suggested that more research and analysis on this matching might be needed.

On a separate technical issue, law enforcement participants noted issues with IP address assignment and attribution. Participants noted that blocks of IP addresses are often reassigned or subleased to other providers, which makes it difficult for law enforcement to identify the correct ISP to contact with queries or legal process related to particular web addresses. It was noted that, for similar issues involving telephone numbers, the company Neustar has a service that maintains an up-to-date list of which provider manages or monitors a particular phone number, and participants discussed whether such a service for IP addresses could be useful (Neustar Communications, undated). Ultimately, participants suggested that the ECPA's provisions prohibiting voluntary disclosure of customer communications to government entities may be a roadblock to simply seeking out the provider to serve with legal process for access to a particular IP address. Participants also suggested that research on the subject may be beneficial.

A portion of the technical discussion was spent talking about law enforcement issues with smart systems and IoT

Table 4. Needs Related to Extraterritorial Evidence and the MLAT Process

Problem or Opportunity	Associated Needs
Data and information about the throughput of the MLAT process are extremely difficult to obtain.	<ul style="list-style-type: none"> • Provide financial, technical, or professional support to the development of the MLAT "online docket" that DOJ OIA has been considering. • Conduct research and analysis on existing or future data on the DOJ OIA MLAT process.
There is no central repository that helps investigators identify the legal standard that needs to be met and the process for making the request.	<ul style="list-style-type: none"> • Ask relevant experts with websites (e.g., DOJ OIA or MLAT.info) to publish additional information that investigators would find useful.
There is a small number of countries that do not have MLATs with the United States and a larger number that do not have them with each other.	<ul style="list-style-type: none"> • Conduct research on the current state of affairs and the associated risks and benefits of expanding the international MLAT regime.
Foreign legal liaisons assigned to the United States on behalf of their countries often appear to be insufficiently informed about the basics of the U.S. legal system.	<ul style="list-style-type: none"> • Conduct research to assess the deficit and liaise with U.S. trainers who are already focused on training foreign nationals on U.S. law.

devices. It was generally agreed that many of the new, connected devices that have been proliferating rapidly could generate data that might be useful as evidence in cases (i.e., might have evidentiary utility). Participants noted, for example, that Carfax, Hertz, and other vehicle-related companies collect vehicle histories, including oil changes, vehicle locations, and potentially even snapshots from an in-car camera that could have evidentiary utility.¹² However, for many of the law enforcement participants, most of these devices remained something of a “black box.” Participants noted that it is difficult to know or keep up to date on what data or metadata are being stored or transmitted by these devices, the manner in which this data could be extracted, the legal requirements for their acquisition (e.g., a warrant), or the company or point of contact to reach out to in individual cases. While some participants suggested solutions, like an information exchange for investigators to share information on IoT devices or manufacturer surveys to catalog device information, other participants were skeptical of the efficacy of some of these solutions. Much of this information would be considered proprietary, and efforts to discover and catalog it may meet significant industry resistance. One participant later commented that a catalog of companies and points of contact for various devices should be feasible, but cataloging information on data types would likely be much more difficult because of claims of proprietary data. Needs related to technical issues are provided in Table 5.

Consolidating Needs

Following these discussions, the last brief session was spent going through the generated list of identified needs and solutions. Participants reviewed the list and were asked to fill in missing needs or solutions, review and approve questionable pairs, and assess whether anything had been missed in each section. A broad assessment was also made of the subjects that had been of most interest to participants. Ultimately, foreign data localization mandates ended up not being a major concern for many of the attendees. It was a backdrop to many of the discussions, as a negative outcome that could become a problem if

¹² It should also be noted that data originating from any devices, including IoT devices, in places with a special legal expectation of privacy, such as in a home or vehicle, probably require a warrant based on probable cause for law enforcement to obtain access. Data originating from a location without expectation of privacy might require lesser legal process, such as a court order or subpoena, depending on what status the data have under the definitions specified in the ECPA.

some of the issues under discussion, such as the MLAT process, were not fixed, but few participants noted immediate concerns over it. Perhaps unsurprisingly, given the central third-party role of service providers in this context, issues related to law enforcement and service provider cooperation made up a significant proportion of the workshop discussion, in addition to related frustrations with U.S. law and procedure.

After the needs had been refined and consolidated into a final list, participants were briefed on the methods being used for needs prioritization and the workshop proceeded to the final prioritization of the needs.

PRIORITIZED NEEDS

The needs discussed were identified as important problems and associated solutions for practitioners and other stakeholders and are thus each worthy of consideration by the community. However, for those organizations that need information to make trade-off decisions when deciding where to focus their resources, a prioritized list can be extremely helpful. As such, following the workshop discussion, the panel attendees were asked to engage in a needs prioritization session. A detailed description of the methodology for the prioritization is given in the appendix to this report. Briefly, participants were asked to rate each need in terms of expected impact and likelihood of success. The combination of these two factors led to a ranked list of the needs, which will be discussed in this section.

Prioritized Needs for Digital Evidence Held in Remote Data Centers

The panel discussion ultimately identified 36 needs that could offer improvements for law enforcement, providers, and other stakeholders on the issue of digital evidence held in remote data centers. From the list of 36 needs, six needs emerged as high-priority or top-tier needs after the prioritization. Top-tier needs are presented in Table 6, and middle-tier and lower-tier needs are presented in Tables 7 and 8, respectively.

The development of databases and information-sharing systems for points of contact (POC) and information on devices, apps, and service provider systems were consistently identified as high-priority needs. Several of the top-tier needs relate to these subjects. These needs were identified both as very likely to help and as very easy to accomplish. Participant comments noted that miscommunication or lack of communication

Table 5. Needs Related to Technical Issues

Problem or Opportunity	Associated Needs
<p>Smart vehicles and other IoT devices collect and transmit information that has evidentiary utility, but it is difficult to identify which data are being retained and identify the appropriate point of contact to serve legal process.</p> <p>There are a variety of app ecosystems that maintain data, but in these cases, it is much harder to identify the point of contact to serve legal process and to know which data are being retained.</p>	<ul style="list-style-type: none"> • Develop an information exchange system where investigators can share information on points of contact and the types of data collected by the devices and apps.
<p>The methodologies for acquiring evidence are constantly evolving.</p>	<ul style="list-style-type: none"> • Incentivize the research community to conduct activities that keep the knowledge base current (grants, conferences, etc.).
<p>There is an access deficit for state and local agencies to perform facial recognition matches in a centralized database (e.g., FBI).</p> <p>There is an access deficit for state and local agencies to search latent prints in the FBI's database.</p>	<ul style="list-style-type: none"> • Enable access for all state and local agencies through the FBI.
<p>Agencies are under strain with respect to cost and capacity for storage and sharing of photographic, video, and digital evidence.</p>	<ul style="list-style-type: none"> • To inform practitioner decisionmaking, develop a cost and efficiency best practices guide for "bulk" storage, retrieval, and sharing of digital evidence.
<p>There is an access deficit for state and local agencies to perform facial recognition matches in a centralized database (e.g., FBI).</p> <p>There are a variety of smart systems that transmit information that has evidentiary utility. It is difficult to identify which data are being retained.</p>	<ul style="list-style-type: none"> • Fund development of a universal face workstation and the software to launch the searches. • Survey manufacturers and/or conduct laboratory research and catalog the kinds of information these devices collect.
<p>It is difficult to audit or verify that the evidence that was provided is, in fact, an accurate extraction of the relevant information in the providers' systems.</p>	<ul style="list-style-type: none"> • Conduct research and interviews with CJIS and FEDRAMP certifiers to explore their willingness to examine the procedures for information extraction.

NOTE: CJIS = Criminal Justice Information Services. FEDRAMP = Federal Risk and Authorization Management Program.

between law enforcement and providers was involved in most disputes related to evidence requests, and anything that could make such communication easier or clearer would be helpful. One participant commented that the need to develop an information exchange system for investigators to share information on POCs and data types, in particular, "appears to be an easy fix with a big payoff." Despite this, some participants were skeptical about sharing information from providers where proprietary data may be involved because providers would likely push back, decreasing the chance of success. Indeed, concerns about resistance from providers in situations where proprietary data or information on provider systems may be concerned were raised in many of the needs. Caveats were also noted on efforts to keep the knowledge base current for evidence acquisition methodologies or procedures for serving legal process. Participants commented that such efforts would be laudable, but, ultimately, a "statutory fix is needed at the state or federal level" for "confusing or outdated laws." For the needs of the development of better standards for officers and providers and better

standardized online training, participants commented that the key to the success of such efforts would be keeping these things updated and that simply making them available might be inadequate, given different learning styles and aptitude among officers for online self-study.

The majority of the identified needs related to improvements in the MLAT system were ranked within the middle tier. While these needs were consistently highly ranked in terms of potential impact, the lower prioritization is the result of somewhat lower participant rankings for likelihood of success. Participants made such comments as "DOJ must own this issue and constantly refresh the information"; "this is a DOJ issue"; and "I am convinced that the baseline MLAT system can be much improved, but ultimately the problem is political" to explain their lower ranking for feasibility. This pessimism notwithstanding, most of the needs related to improving the MLAT process were among the most highly ranked within the middle tier of identified needs.

Table 6. Top-Tier Needs Related to Digital Evidence Held in Remote Data Centers

Problem or Opportunity	Associated Needs
There is no database for contact information for specialists who deal with remote digital evidence.	<ul style="list-style-type: none"> • Create a database or portal where law enforcement can access contact information, documentation, and training for accessing remote digital evidence.
Investigators are often unaware of the kinds of information that can be requested and the options for bounding their requests.	<ul style="list-style-type: none"> • Develop standardized online training for investigators to assist with requesting evidence and data.
<p>Smart vehicles and other IoT devices collect and transmit information that has evidentiary utility, but it is difficult to identify which data are being retained and the appropriate point of contact to serve legal process.</p> <p>There are a variety of app ecosystems that maintain data, but in these cases, it is much harder to identify the point of contact to serve legal process and to know which data are being retained.</p>	<ul style="list-style-type: none"> • Develop an information exchange system where investigators can share information on POCs and the types of data collected by the devices and apps.
The methodologies for acquiring evidence are constantly evolving.	<ul style="list-style-type: none"> • Incentivize the research community to conduct activities that keep the knowledge base current (grants, conferences, etc.)
Finding the contact information and communicating with providers' legal representatives can be extremely difficult.	<ul style="list-style-type: none"> • Develop an information exchange system where investigators can share information on POCs and the types of data that are available via different providers.
Procedures for serving legal process are often not well defined or are unclear.	<ul style="list-style-type: none"> • Develop standards that are easier for providers and investigators to comply with.

Table 7. Middle-Tier Needs Related to Digital Evidence Held in Remote Data Centers

Problem or Opportunity	Associated Needs
Data and information about the throughput of the MLAT process are extremely difficult to obtain.	<ul style="list-style-type: none"> • Provide financial, technical, or professional support to the development of the MLAT online docket that DOJ OIA has been considering. • Conduct research and analysis on existing or future data on the DOJ OIA MLAT process.
Investigators are often unaware of the kinds of information that can be requested and the options for bounding their requests.	<ul style="list-style-type: none"> • Develop an online repository (i.e., a clearinghouse) for best practices in making digital evidence requests.
It can be difficult for an agency in one state to obtain a warrant to get data from a provider in another state—judges often do not feel that they have the authority.	<ul style="list-style-type: none"> • Conduct research on model statutes that could improve the procedures for serving and responding to legal process. • Develop a Turbo Tax–like system for preparing warrants that are compliant with the appropriate jurisdiction.
It is often difficult to determine which jurisdiction has the authority to compel production of the data and, thus, where the legal process or MLAT should be served.	<ul style="list-style-type: none"> • Facilitate the development of a uniform system of jurisdiction over data in the cloud.
Search warrant parameters imposed by judges are often not aligned with the technical limitations of the systems and devices being searched.	<ul style="list-style-type: none"> • Develop an information exchange system where investigators can share information on points of contact and best practices for search warrant design.
<p>There is an access deficit for state and local agencies to perform facial recognition matches in a centralized database (e.g., FBI).</p> <p>There is an access deficit for state and local agencies to search latent prints in the FBI's database.</p>	<ul style="list-style-type: none"> • Enable access for all state and local agencies through the FBI.

Table 7—Continued

Problem or Opportunity	Associated Needs
There is not a central repository that helps investigators identify the legal standard that needs to be met and the process for making the request.	<ul style="list-style-type: none"> • Ask relevant experts with websites (e.g., DOJ OIA, MLAT.info) to publish additional information that investigators would find useful.
There can be a misalignment between the way that data are requested and the way that they are stored. Without sufficient communication or specification between the requestor and the provider, the result can be unhelpful.	<ul style="list-style-type: none"> • Conduct research and interviews on what service providers are willing to do to facilitate the exchange of information that should legitimately be provided in response to legal process.
Blocks of IP addresses are often reassigned or subleased to other providers, making it difficult to identify the actual ISP with the customer relationship.	<ul style="list-style-type: none"> • Conduct research and analysis to highlight the impact on law enforcement with regard to ECPA's prohibition of voluntary disclosure of customer communications records to government entities (U.S.C. 2702(a)(3)).
A large number of cybercrimes cannot effectively be investigated using local resources (e.g., ransomware attacks).	<ul style="list-style-type: none"> • Evaluate the efficacy of specialized task forces focused on lower-level cybercrimes.
There is a small number of countries that do not have MLATs with the United States and a larger number that do not have them with each other.	<ul style="list-style-type: none"> • Conduct research on the current state of affairs and the associated risks and benefits of expanding the international MLAT regime.
The requests made by law enforcement are often difficult or impossible for data custodians (i.e., providers) to comply with.	<ul style="list-style-type: none"> • Develop curricula and training materials that help law enforcement trainers construct requests that are more technically feasible (and are potentially reviewed by provider industry groups).
Data custodian procedures frequently change, which often frustrates law enforcements' ability to reuse previously successful procedures.	<ul style="list-style-type: none"> • Develop a standard for law enforcement requests to industry for user data.
Foreign legal liaisons assigned to the United States on behalf of their countries often appear to be insufficiently informed about the basics of the U.S. legal system.	<ul style="list-style-type: none"> • Conduct research to assess the deficit and liaise with existing U.S. trainers who are already focused on training foreign nationals on U.S. law.
There are few published "how-to" procedures that practitioners can follow to request data from data custodians (i.e., providers). Thus, the learning curve can be very steep for investigators who are not familiar with current processes.	<ul style="list-style-type: none"> • Develop a "50-state guide" on search warrant procedures (if it does not already exist).

Table 8. Lower-Tier Needs Related to Digital Evidence Held in Remote Data Centers

Problem or Opportunity	Associated Needs
<p>There is a lack of financial incentives for service providers when attempting to comply with legal process inquiries.</p> <p>There are no standards for data retention.</p>	<ul style="list-style-type: none"> • Catalog the difficulties the service providers experience when attempting to comply with legal process. • Develop a catalog of existing industry practices (as a means of informing investigators and potentially suggest a common guideline or standard).
<p>Agencies are under strain with respect to cost and capacity for storage and sharing of photographic, video, and digital evidence.</p>	<ul style="list-style-type: none"> • To inform practitioner decisionmaking, develop a cost and efficiency best practices guide for “bulk” storage, retrieval, and sharing of digital evidence.
<p>Even when the investigators follow the appropriate processes, they might still have difficulty obtaining the data that they requested and have the authority to obtain.</p>	<ul style="list-style-type: none"> • Conduct research to assess the risks and benefits of domestic and international sanction regimes.
<p>A large number of cybercrimes cannot effectively be investigated using local resources (e.g., ransomware).</p>	<ul style="list-style-type: none"> • Develop a standard set of vetted resources (e.g., nomoreransom.org) that can be shared via agency websites.
<p>It is difficult to make contact with experienced investigators from other agencies who have recent or relevant experience with requesting data or evidence.</p>	<ul style="list-style-type: none"> • Suggest that professional organizations (e.g., state attorneys general, IACP) collectively examine the issue and produce templates for search warrants and the office(s) to submit them to.
<p>There is an access deficit for state and local agencies to perform facial recognition matches in a centralized database (e.g., FBI).</p>	<ul style="list-style-type: none"> • Fund development of a universal face workstation (and the software to launch the searches).
<p>Provider data formats are often not machine-readable, and tools are not provided to read them.</p>	<ul style="list-style-type: none"> • Develop best-practice boilerplate language for requesting data. For example, they should be in a native format or file and machine-readable; if the format is proprietary, a reader/decoder should also be supplied.
<p>It is still difficult to know where to serve legal process to obtain user data inside the United States.</p>	<ul style="list-style-type: none"> • Develop a guide to educate providers and device manufacturers on how law enforcement prefers to request data and interact.
<p>There are a variety of smart systems that transmit information that has evidentiary utility. It is difficult to identify which data are being retained.</p>	<ul style="list-style-type: none"> • Survey manufacturers and/or conduct laboratory research and catalog the kinds of information these devices collect.
<p>The methodologies for acquiring evidence are constantly evolving.</p>	<ul style="list-style-type: none"> • Develop model statutes for federal, state, and local legislatures that are often updated to address the current state of technology.
<p>There is a lack of clarity on providers’ interpretation of jurisdiction over their legal organizational architecture and the choices they have made to ensure data residency and jurisdiction.</p>	<ul style="list-style-type: none"> • Conduct research and analysis on provider information technology/organizational architecture and the implications for U.S. and foreign jurisdiction.
<p>It is difficult to audit or verify that the evidence provided is, in fact, an accurate extraction of the relevant information in the providers’ systems.</p>	<ul style="list-style-type: none"> • Conduct research and interviews with CJIS and FEDRAMP certifiers to explore their willingness to also examine the procedures for information extraction.

Many of the needs in the middle tier were also related to improving the processes and methodologies for acquiring data from other states. Several involved helping investigators write better data requests to providers and obtain warrants for data in other jurisdictions, while others concerned the clarification of authority to do so. Participant comments touched on the idea of improving a uniform act for cross-state requests to make them less time consuming. Likewise, several others mentioned the need for a legislative solution for such problems. Again, enthusiasm for the impact of such solutions was tempered by lower expectations of the likelihood of success, largely because of the perceived need for a legislative solution. On the need to facilitate the development of a uniform system of jurisdiction over data in the cloud, one participant commented that “a uniform system would have a huge payoff, but would be very difficult to put together,” and one participant went so far as to comment “this is the holy grail, but it is so unrealistic that, in my honest opinion, it is not worth pursuing.” Such perceptions from participants led to lower rankings for likelihood of success, resulting in several needs with high perceived impact nevertheless ending up in the middle tier.

CONCLUSION

Digital evidence held in remote data centers will play an increasingly significant role in law enforcement investigations. Law enforcement at all levels, from federal to state and local investigators, will need adequate training to access and use digital evidence that may reside hundreds or thousands of miles away across state or national boundaries. The ubiquity of digital data and their integration into our daily lives, coupled with the growth of remote cloud storage, means that investigators must have access to these data in routine investigations. The systems and legal authority that law enforcement must operate within to perform their investigations, however, have not kept pace with the changes in technology, and law enforcement officers are facing barriers, decreasing their ability to successfully investigate crimes.

The routine storage of such data as emails, which users seamlessly access from their personal devices, in data centers across the country or outside it, means that officers are more regularly confronted with the complexity and legal ambiguity of requesting these data from remote third parties. While the device used to access these data may be local, the investigation must span borders, and workshop participants discussed the

significant challenges associated with this process. Laws made before the rise of the modern global internet present practitioners with ambiguity on the appropriate means of serving legal process and uncertainty on the authority to request data. Even when data reside within the United States, practitioners often face challenges in determining what data are available, what individual or organization to serve legal process to, and how to appropriately bound their data requests. When the data are outside the United States, they must be requested through the MLAT process, which is insufficiently transparent and so time consuming that some practitioners perceive it as an insurmountable barrier for routine digital evidence requests. While some legislative solutions to these problems have been proposed, reforms have not yet been enacted. Workshop participants discussed many of these problems and the nonlegislative needs that offer potential improvements.

As the quantity of stored digital data has grown, the relationship between law enforcement and service providers has also changed. The burdens imposed by the volume and complexity of law enforcement data requests and the integral role of service providers in the acquisition of that data by investigators have morphed these providers from true third parties to stakeholders in the process. Even when practitioners successfully navigate sometimes ambiguous or time-consuming processes in the course of their investigations, they are often stymied by an adversarial relationship with service providers. Workshop participants discussed the perspectives of both law enforcement and service providers to determine the means of easing burdens and to improve cooperation.

The workshop identified high-priority needs through the Delphi Method (RAND Corporation, 2017). The highest-priority needs were aligned with the topics identified in pre-workshop surveys and the literature review. The high-priority needs touched on the following topics:

- *Creation of a portal or database for the sharing of information.* Participants thought that many of the difficulties encountered by investigators could be mitigated by better access to information. A portal, database, or information exchange of some kind was proposed as a means of facilitating ease of access to contact information for specialists in remote digital evidence acquisition and training for investigators on the creation and appropriate bounding of requests to providers for data. Such a portal was also suggested as a repository of information on POCs with service providers, types of data and formats used by common

providers, and types of data used by various apps and IoT devices.

- *Better standards for data requests.* Participants identified a need for better standards for the creation of and compliance with data requests served to providers. This was intended as a means of providing all stakeholders with a common picture of what is required in serving and complying with legal process. It would clarify the expectations of law enforcement and providers, remove ambiguity about the appropriate process or response, and mitigate investigative delays or unnecessary compliance burdens.
- *More research on methodologies for collecting digital evidence.* Participants noted that the methodologies for digital evidence collection are constantly changing, and there is a need for the research community to keep the knowledge base current. This could be facilitated with greater incentives for research in this area, such as targeted grants and conferences dedicated to the subject. Such incentives would help the research community keep pace with the persistent influx of new data types and devices.
- *Improved communication with service providers.* Investigators need to know who to talk to, what data they have, and what information researchers need to include in the request to better understand what data are required and make it as technically simple to comply with as possible.
- *Improvements in the MLAT process.* Participants noted that many changes for the MLAT process have been proposed, but a helpful first step would likely be researching the specific bottlenecks in the process that need to be targeted for improvement. Other identified needs touched on better training for foreign liaisons who handle requests, portals to provide stakeholders with visibility into the state of requests, and fixing gaps in the system where countries have no legal means of sharing evidence.
- *Improvements for interstate data requests.* Participants found there to be ambiguous legal authority and insufficient training for requesting data from other states. Officers noted that providers had varying expectations on the types of legal process they would accept from an agency in another state, and both investigators and judges were often unclear on their authority to make requests across state lines. Participants wanted published standards and “how-to” guides to clarify the needs and authority for interstate data requests.

All stakeholders in the process face challenges in the acquisition of digital evidence held in remote data centers, and this prioritized list of needs offers a valuable set of first steps and priorities on which to focus to facilitate a more effective process for all parties.

APPENDIX: TECHNICAL METHODS

This appendix presents additional detail on the panel process, needs identification and prioritization carried out to develop the research agenda presented in the main report. The text in this appendix draws heavily on similar descriptions in Hollywood, Boon, et al., 2015; Hollywood, Woods, et al., 2015; and Jackson et al., 2015.

Pre-Workshop Activities

RAND and the Police Executive Research Forum (PERF) recruited the panel members by extending invitations to knowledgeable individuals identified through existing professional and social networks (e.g., LinkedIn) and by reviewing literature published on the topic. At the time of the invitation, panelists were provided with a brief description of the workshop’s focus areas.

To prepare for the workshop, panelists were provided with read-ahead materials via email and were given an opportunity to identify the issues and topics that they felt would be important to discuss. The read-ahead document is discussed in the main report. Prior to the workshop, 23 attendees responded with feedback regarding the topics they deemed worthy of further discussion.

Panelist responses with regard to matters of procedure and law are displayed in Figure A.1. Panelists were asked to rank six matters of procedure and law on a scale of one to ten for both importance and difficulty. Panelists generally agreed that the ability to access and collect the “right” evidence was the most important matter. Accessing and collecting evidence was the task that the panelists found to be the most difficult to accomplish.

Panelist responses to technical matters are displayed in Figure A.2. Panelists agreed that the ability to analyze and present evidence was extremely important but did not generally agree about how difficult it was to perform. Agreement was not as strong for the other technical matters in terms of importance, but the panelists generally agreed that all of these items were

important. The panelists generally agreed that dealing with foreign data localization mandates was the most difficult task, while the levels of agreement on the difficulty of other tasks were not as significant.

The quantitative responses summarized in Figure A.1 and Figure A.2, as well as the narrative responses that catalogued particular pain points (areas of need) and other suggested areas of difficulty, were used by the discussion moderator to guide the discussion during the in-person panel.

The workshop agenda is presented in Table A.1.

Prioritization of Needs

During the workshop, participants collectively reviewed the list of “pain points” and issues that they individually provided prior to the workshop. While conducting this review, they suggested additional areas worthy of potential research or investment. Workshop participants also considered whether there were areas

that were not included in the existing list and suggested new ones.

To develop and prioritize a list of technology and policy areas that are likely to benefit from research and development investment, we followed a process that has been used in previous research (see, for example, Jackson et al., 2016, and references therein). The panelists discussed and refined issues and problems in each category and also identified potential needs (e.g., solutions). Once the group had compiled and refined its list of issues and needs, they were converted into a web-based Delphi instrument (using the Qualtrics service).

Using the instrument, each panelist was asked to individually score each issue and its associated need using a 1–9 scale for the following dimensions: (1) importance or payoff and (2) probability of success. For the importance or payoff dimension, participants were instructed that 1 was a “low” score and 9 was a “high” score. Participants were further told to score the importance or payoff dimension with a 1 if the need or solution would have little or no impact on the problem and with a 9 if

Figure A.1. Panel Assessment of Matters of Procedure and Law

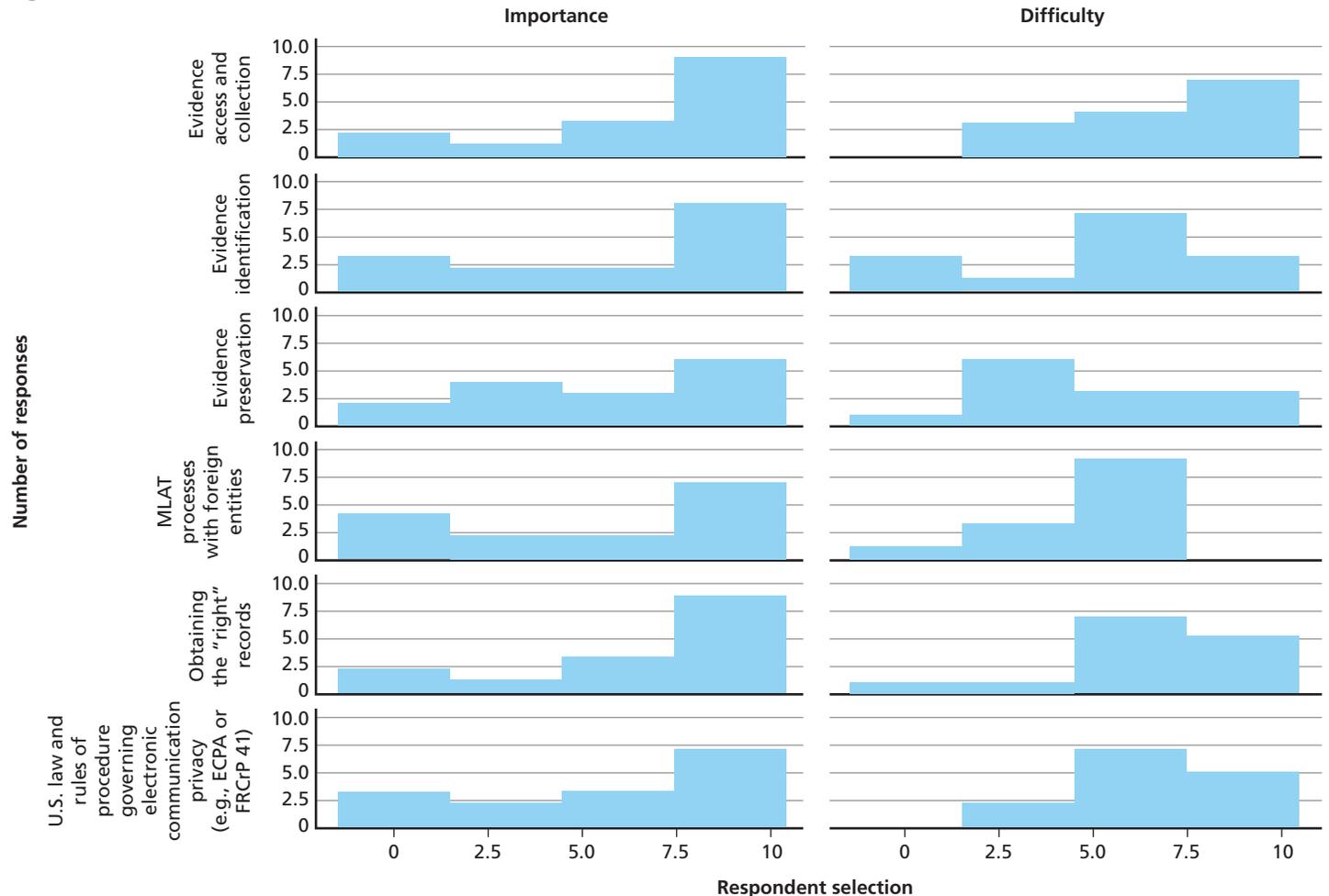


Figure A.2. Panel Assessment of Technical Matters

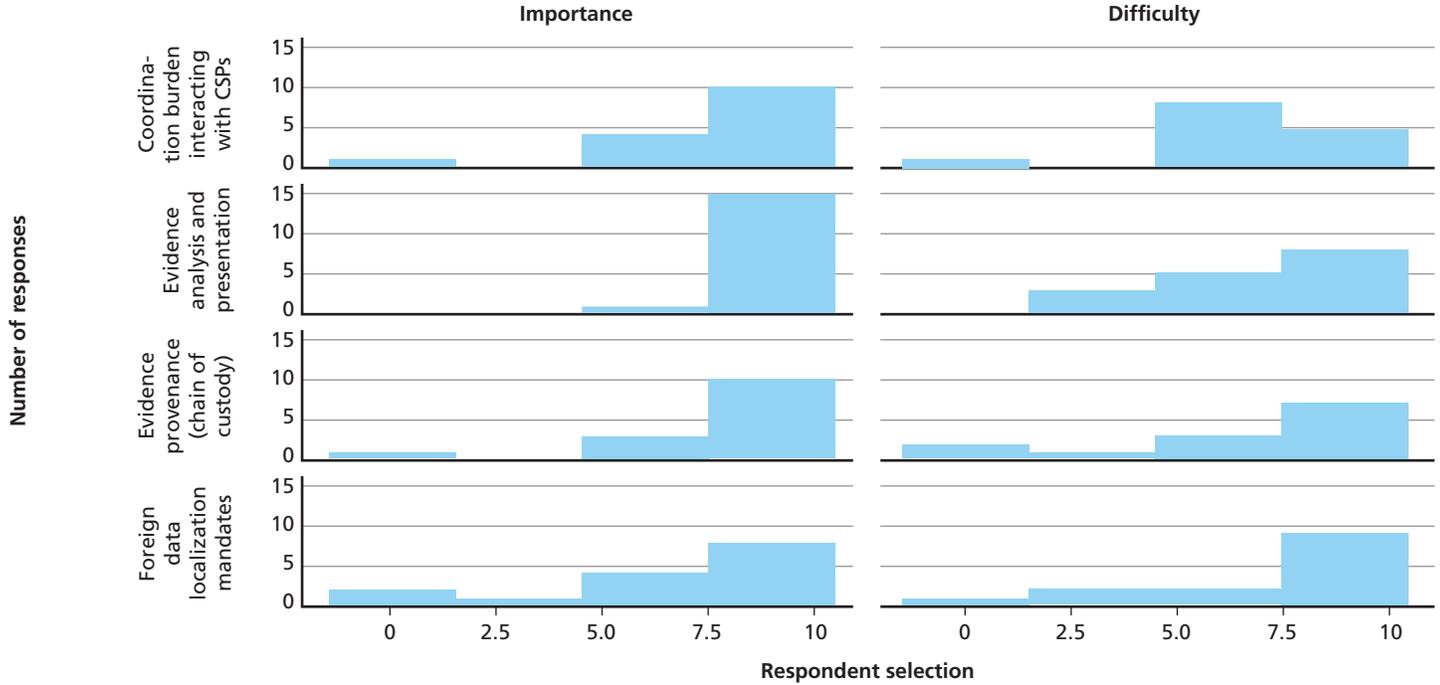


Table A.1. Workshop Agenda

Day 1		Day 2	
8:30	Welcome and Introductions	8:30	Needs Discussion
9:30	Needs Discussion	10:30	Review and Final Brainstorming
11:30	Lunch	11:30	Working Lunch
1:00	Needs Discussion	12:00	Prioritize Needs
5:00	Adjourn	1:30	Wrap-up and Next Steps
		2:00	Adjourn

the need or solution would reduce the impact of the problem by 20–30 percent (or more).

When the first Delphi round was completed, the panel’s responses and comments were anonymously collected and summarized. The summary contained a “kernel density” distribution figure and a summary of the panel’s comments for each issue and need. This summary was used to facilitate discussion among the panelists on the needs that had the most disagreement either in the area of payoff or in the probability of success. The purpose of the discussion was to encourage the panelists to discuss their differences and to attempt to move toward consensus. During each discussion, panelists were asked to return to the Delphi tool to provide a second round of responses while

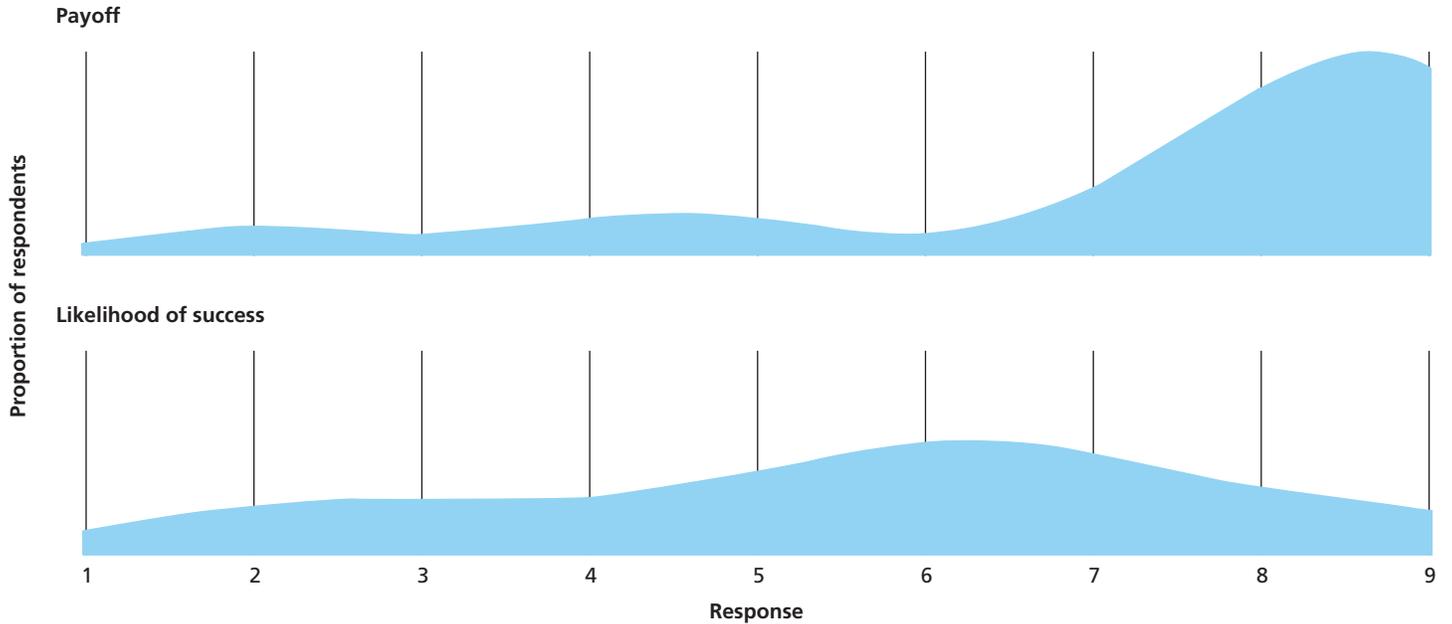
keeping the group’s collective response and any discussion in mind.¹³

Figure A.3 is an example of one of the needs presented to the group prior to providing their second-round answers:

- **Issue:** A large number of cybercrimes (e.g., ransomware) cannot effectively be investigated using local resources.
- **Need:** Develop a standard set of vetted resources (e.g., nomoreransom.org) that can be shared via agency websites.
- **Comments:**

¹³ Due to a technical difficulty, nine questions were not presented to the respondents during the in-room session. To address this, a Delphi instrument containing the missing questions was emailed to the participants after the workshop. Approximately half of them responded, and their responses were directly integrated into the overall list of prioritized responses.

Figure A.3. Example Post-Round 1 Delphi Summary Question



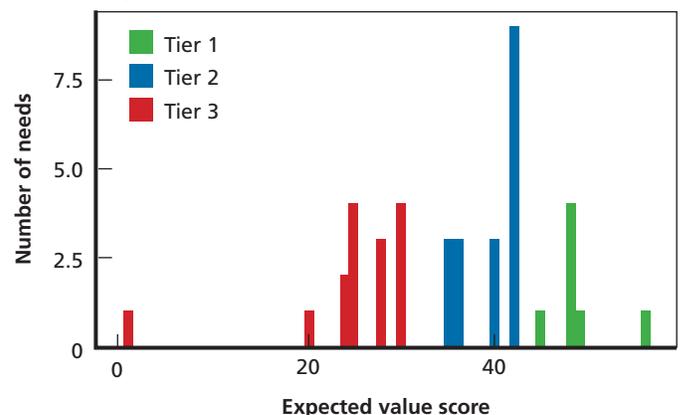
- This will become increasingly important as more IoT technology develops
- The POC issue is highly solvable. Handling the wide variety of data types will probably be harder.

Once the round 2 responses were collected, they were ranked by calculating an expected value using the method outlined in Jackson et al., 2016. Specifically, for each question, the payoff and the likelihood of success were multiplied together, and the median of that product was the expected value. Instead of providing an individually rank-ordered list of priorities, we chose to cluster the list of needs into three tiers. We did this because the small sample size and level of uncertainty resulting from the abstract nature of the ranking process do not result in highly precise rank-orderings. Furthermore, the purpose of the list of needs is to provide policymakers and technology developers with a sense of what set of priorities would be most valuable for further investment. Thus, the precise numerical ranking is not used directly, but instead those items that rose to the “top” are carried forward for additional action. As such, the primary result from the clustering process is to identify the best place to locate the cutoff where the highest-priority group of needs ends and the lower-priority groups begin.

To cluster the expected values, we used a hierarchical clustering algorithm. Specifically, the algorithm that was selected was the “ward.D” spherical algorithm from the “stats” library in the R statistical package, version 3.4.1. We prefer it for this purpose to minimize within-cluster variance when determining

the breaks between tiers. The choice of three tiers is arbitrary but was done in part to remain consistent across the set of technology workshops conducted for NIJ. Also, the choice of three tiers represents a manageable system for policymakers. Specifically, the top tier contains the priorities that should be the primary policymaking focus; the middle tier can and should be examined closely; and the final tier is probably not worth much attention in the short term. Figure A.4 shows the distribution of the needs by the expected value score. The height of the bar indicates the number of needs that had that score, and the color of the bar indicates the tier that the need was ultimately assigned to by the clustering algorithm.

Figure A.4. Distribution of the Clustered Needs Following Round 2



BIBLIOGRAPHY

- Access, “Mutual Legal Assistance Treaties: Discussion Paper: What is Wrong with the International System for Sharing Online Records for Criminal Matters,” webpage, 2017a. As of February 21, 2018: <https://mlat.info/policy-analysis-docs/what-is-wrong-with-the-mlat-system>
- Access, “Mutual Legal Assistance Treaties: Frequently Asked Questions,” webpage, 2017b. As of February 21, 2018: <https://mlat.info/faq>
- Accenture, “Building Digital Trust: The Role of Data Ethics in the Digital Age,” 2016. As of February 21, 2018: <https://www.accenture.com/us-en/insight-data-ethics>
- Alqahtany, Saad, Nathan H. Clarke, Steven Furnell, and Christoph Reich, “Cloud Forensics: A Review of Challenges, Solutions, and Open Problems,” *Proceedings of the 2015 International Conference on Cloud Computing*, 2015, pp. 1–9.
- Blanco, Kenneth, “An Important Court Opinion Holds Lawful Warrants Can Be Used to Obtain Evidence from U.S. Internet Service Providers When Those Providers Store Evidence Outside the U.S.,” U.S. Department of Justice, February 6, 2017. As of February 21, 2018: <https://www.justice.gov/opa/blog/important-court-opinion-holds-lawful-warrants-can-be-used-obtain-evidence-us-internet>
- Cauthen, John M., “Executing Search Warrants in the Cloud,” FBI Law Enforcement Bulletin, October 7, 2014. As of February 21, 2018: <https://leb.fbi.gov/2014/october/executing-search-warrants-in-the-cloud>
- Chander, Anupam, and Uyen P. Le, “Breaking the Web: Data Localization vs. the Global Internet,” California International Law Center, Research Paper No. 378, April 2014.
- Chertoff Group, *Law Enforcement Access to Evidence in the Cloud Era*, Washington, D.C., 2015. As of February 21, 2018: <https://www.chertoffgroup.com/files/docs/LawEnforcement.pdf>
- Daskal, Jennifer, “The Un-Territoriality of Data,” *Yale Law Journal*, Vol. 125, No. 2, November 2015, pp. 326–559.
- Daskal, Jennifer, and Andrew K. Woods, “Cross-Border Data Requests: A Proposed Framework,” *Just Security*, November 24, 2015. As of February 21, 2018: <https://www.justsecurity.org/27857/cross-border-data-requests-proposed-framework/>
- Del Greco, Kimberly J., Law Enforcement’s Use of Facial Recognition Technology, Statement before the Committee on Oversight and Government Reform, U.S. House of Representatives, March 22, 2017. As of February 21, 2018: <https://oversight.house.gov/wp-content/uploads/2017/03/Del-Greco-FBI-Statement-FRT-Study-3-22.pdf>
- Digital Due Process Coalition, “About the Issue: ECPA Reform: Why Now?” webpage, 2017. As of February 21, 2018: <https://digitaldueprocess.org>
- Dykstra, Josiah, “Seizing Electronic Evidence from Cloud Computing Environments,” in Keyun Ruan, ed., *Cybercrime and Cloud Forensics: Applications for Investigation Processes*, IGI Global, 2013, pp. 156–185.
- Dykstra, Josiah, and Alan T. Sherman, “Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing: Exploring and Evaluating Tools, Trust, and Techniques,” *Digital Investigation*, Vol. 9, 2012, pp. S90–S98.
- EEOC v Arabian American Oil Co.*, 499 (U.S. 233, 248), 1991.
- Electronic Frontier Foundation, *Who Has Your Back?* San Francisco, Calif., 2017.
- Fox-Brewster, Thomas, “Inside Google’s Fight to Keep the U.S. Government out of Gmail Inboxes,” *Forbes*, May 21, 2017. As of February 21, 2018: <https://www.forbes.com/sites/thomasbrewster/2017/05/21/google-epic-court-fight-with-us-government-over-gmail-privacy>
- Goodison, Sean E., Robert C. Davis, and Brian A. Jackson, *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*, Santa Monica, Calif.: RAND Corporation, RR-890-NIJ, 2015. As of February 21, 2018: https://www.rand.org/pubs/research_reports/RR890.html
- Google Inc., “Transparency Report: Requests for User Information,” 2017. As of February 21, 2018: <https://google.com/transparencyreport/userdatarequests>
- Hogan Lovells, “*Marco Civil da Internet*: Brazil’s New Internet Law Could Broadly Impact Online Companies’ Privacy and Data Handling Practices,” webpage, undated. As of February 21, 2018: <http://ehoganlovells.com/cv/92a5426dc5d9947a6ef3abd4eb988b549ae2472b>
- Hollywood, John S., John E. Boon, Jr., Richard Silbergliitt, Brian G. Chow, and Brian A. Jackson, *High-Priority Information Technology Needs for Law Enforcement*, Santa Monica, Calif.: RAND Corporation, RR-737-NIJ, 2015. As of February 21, 2018: https://www.rand.org/pubs/research_reports/RR737.html
- Hollywood, John S., Dulani Woods, Richard Silbergliitt, and Brian A. Jackson, *Using Future Internet Technologies to Strengthen Criminal Justice*, Santa Monica, Calif.: RAND Corporation, RR-928-NIJ, 2015. As of February 21, 2018: https://www.rand.org/pubs/research_reports/RR928.html
- “How Much Is Your Gmail Account Worth?” *Wired*, July 25, 2012. As of February 21, 2018: <http://www.wired.com/insights/2012/07/gmail-account-worth>
- IACP—See International Association of Chiefs of Police.

International Association of Chiefs of Police, *Data, Privacy, and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence*, Alexandria, Va., 2015.

Jackson, Brian A., *Respect and Legitimacy—A Two-Way Street: Strengthening Trust Between Police and the Public in an Era of Increasing Transparency*, Santa Monica, Calif: RAND Corporation, PE-154-RC, 2015. As of February 21, 2018:
<https://www.rand.org/pubs/perspectives/PE154.html>

Jackson, Brian A., Duren Banks, John S. Hollywood, Dulani Woods, Amanda Royal, Patrick W. Woodson, and Nicole J. Johnson, *Fostering Innovation in the U.S. Court System: Identifying High-Priority Technology and Other Needs for Improving Court Operations and Outcomes*, Santa Monica, Calif.: RAND Corporation, RR-1255-NIJ, 2016. As of December 12, 2016:
http://www.rand.org/pubs/research_reports/RR1255.html

Jackson, Brian A., Joe Russo, John S. Hollywood, Dulani Woods, Richard Silbergliitt, George B. Drake, John S. Shaffer, Mikhail Zaydman, and Brian G. Chow, *Fostering Innovation in Community and Institutional Corrections: Identifying High-Priority Technology and Other Needs for the U.S. Corrections Sector*, Santa Monica, Calif.: RAND Corporation, RR-820-NIJ, 2015. As of March 21, 2018:
https://www.rand.org/pubs/research_reports/RR820.html

Jackson, Brian A., and Dulani Woods, *Interactive Tool for Ranking Digital Evidence Needs*, Santa Monica, Calif.: RAND Corporation, TL-175-NIJ, 2015. As of February 21, 2018:
<https://www.rand.org/pubs/tools/TL175.html>

Kerr, Orin S., “The Next Generation Communications Privacy Act,” *University of Pennsylvania Law Review*, Vol. 162, 2014, pp. 373–419.

Kerr, Orin S., “The Fourth Amendment and the Global Internet,” *Stanford Law Review*, Vol. 67, No. 2, 2015, p. 285.

Microsoft Corp. v United States, 829 F.3d 197 (2d Cir. 2016).

Microsoft Corporation, *Data Privacy Day Privacy Survey 2013*, Seattle, Wash., January 2013.

Microsoft Corporation, “Time for an International Convention on Government Access to Data,” blog post, January 20, 2014. As of February 21, 2018:
<https://blogs.microsoft.com/on-the-issues/2014/01/20/time-for-an-international-convention-on-government-access-to-data/>

MLAT.info, homepage, undated. As of March 15, 2018:
<https://www.mlat.info/>

Neustar Communications, “Communications Solutions,” webpage, undated. As of February 27, 2018:
<https://www.communications.neustar/>

Nomoreransom.org, homepage, undated. As of March 15, 2018:
<https://www.nomoreransom.org/en/index.html>

President’s Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of the President’s Review Group on Intelligence and Communications Technologies*, December 12, 2013. As of February 27, 2018;
https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

Rainie, Lee, and Maeve Duggan, *Privacy and Information Sharing*, Washington, D.C.: Pew Research Center, December 2015. As of February 21, 2018:
http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf

RAND Corporation, “Delphi Method,” 2017. As of October 5, 2017:
<https://www.rand.org/topics/delphi-method.html>

Rueter, Thomas J., Memorandum of Decision, *In re Search Warrant No. 16-960-M-01 to Google and In re Search Warrant No. 16-1061-M to Google*, Cases 16-960-M-01 and 16-1061-M, 2017 WL 471564 (E.D. Pa. Feb. 3, 2017). As of February 21, 2018:
<https://www.justice.gov/archives/opa/blog-entry/file/937001/download>

Search.org, homepage, undated. As of March 15, 2018:
<http://www.search.org/>

Taylor, M., J. Haggerty, D. Gresty, and R. Hegarty, “Digital Evidence in Cloud Computing Systems,” *Computer Law & Security Review*, Vol. 26, No. 3, May 2010, pp. 304–308.

Thompson, Richard M., II and Jared P. Cole, *Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA)*, Washington, D.C.: Congressional Research Service, R44036, May 19, 2015. As of February 21, 2018:
<https://fas.org/sgp/crs/misc/R44036.pdf>

U.S. Code, Title 18, Section 2510-22, Electronic Communications Privacy Act, 1986.

U.S. Code, Title 18, Section 2701-2, Unlawful Access to Stored Communications, 1986.

U.S. Code, Title 18, Section 2701-11, Stored Communications Act, 1986.

U.S. Code, Title 18, Section 2702, Voluntary Disclosure of Customer Communications or Records, 2011.

U.S. Code, Title 18, Section 2703, Required Disclosure of Customer Communications or Records, 2011.

United States v Warshak, 631 F.3d 266 (6th Cir. 2010).

U.S. Department of Justice, *FY 2015 Budget Request: Mutual Legal Assistance Treaty Process Reform*, 2014. As of February 21, 2018:
<https://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf>

U.S. House of Representatives, Online Communications and Geolocation Protection Act, 114th Cong., Washington, D.C., H.R. 656, 2015.

U.S. House of Representatives, Email Privacy Act of 2001, 115th Cong., Washington, D.C., H.R. 387, 2017.

U.S. Senate, Law Enforcement Access to Data Stored Abroad Act, 114th Cong., Washington, D.C., S. 512, 2015.

U.S. Senate, International Communications Privacy Act, 114th Cong., Washington, D.C., S. 2986, 2016.

Vedder, Price, Kaufman, and Kammholz, P.C., *Long-Arm Statutes: A Fifty-State Survey*, Chicago, Ill., 2003.

Walden, Ian, *Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent*, London: Queen Mary School of Law, Research Paper No. 74, November 14, 2011.

Wong, Joon Ian, "Here's How Often Apple, Google, and Others Handed Over Data When the U.S. Government Asked for It," *Quartz*, February 19, 2016. As of February 21, 2018: <https://qz.com/620423/heres-how-often-apple-google-and-others-handed-over-data-when-the-us-government-asked-for-it/>

Woods, Andrew K., *Data Beyond Borders: Mutual Legal Assistance in the Internet Age*, Washington, D.C.: Global Network Initiative, January 2015. As of February 21, 2018: <https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf>

Woods, Andrew Keane, "Against Data Exceptionalism," *Stanford Law Review*, Vol. 68, No. 4, April 2016, p. 729.

Wyatt, Edward, and Claire Cain Miller, "Tech Giants Issue Call for Limits on Government Surveillance of Users," *New York Times*, December 9, 2013. As of February 21, 2018: <http://www.nytimes.com/2013/12/09/technology/tech-giants-issue-call-for-limits-on-government-surveillance-of-users.html>

Zawoad, Shams, and Ragib Hasan, "Digital Forensics in the Cloud," *Crosstalk*, September/October 2013. As of February 21, 2018: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.433.8211&rep=rep1&type=pdf>

Acknowledgments

The authors would like to acknowledge the participation and assistance of the members of the Challenges with Digital Evidence Held in Remote Data Centers workshop. This effort would not have been possible without their generous willingness to spend their time participating in the effort. We would also like to acknowledge the contributions of Martin Novak and Steve Schuetz of the National Institute of Justice. The authors also acknowledge the valuable contributions of the peer reviewers of the report, Rebecca Balebako of RAND, Christopher Slobogin of Vanderbilt University Law School, and the anonymous DOJ reviewers.

The RAND Justice Policy Program

The research reported here was conducted in the RAND Justice Policy Program, which spans both criminal and civil justice system issues, with such topics as public safety, effective policing, police-community relations, drug policy and enforcement, corrections policy, use of technology in law enforcement, tort reform, catastrophe and mass-injury compensation, court resourcing, and insurance regulation. Program research is supported by government agencies, foundations, and the private sector.

This program is part of RAND Justice, Infrastructure, and Environment, a division of the RAND Corporation dedicated to improving policy- and decisionmaking in a wide range of policy domains, including civil and criminal justice, infrastructure protection and homeland security, transportation and energy policy, and environmental and natural resource policy.

Questions or comments about this report should be sent to the project leader, Brian A. Jackson at Brian_Jackson@rand.org. For more information about the Justice Policy Program, see www.rand.org/jie/justice-policy or contact the director at justice@rand.org.

About the Authors

Michael J. D. Vermeer is an associate physical scientist at the RAND Corporation. His research focuses on science and technology policy, criminal justice, national security, and emerging technologies and innovation. His recent research involves program evaluation for various organizations both foreign and domestic and within and outside the national security space, as well as the policy, procedure, and technology needs of criminal justice agencies. He received a B.S. from Calvin College and a Ph.D. from Northwestern University.

Dulani Woods is a data science practitioner adept at data acquisition, transformation, visualization, and analysis. He has a master's degree in agricultural economics (applied economics) from Purdue University. His master's thesis was an economic analysis of organic and conventional agriculture using the Rodale Institute's Farming Systems Trial. He began his career as a Coast Guard officer on afloat and ashore assignments in Miami, Fla.; New London, Conn.; and Baltimore, Md.

Brian Jackson is a senior physical scientist at the RAND Corporation. His research focuses on criminal justice, homeland security, and terrorism preparedness. His areas of examination have included safety management in large-scale emergency response operations, the equipment and technology needs of criminal justice agencies and emergency responders, and the design of preparedness exercises.

About This Report

On behalf of the U.S. Department of Justice, National Institute of Justice (NIJ), the RAND Corporation, in partnership with the Police Executive Research Forum (PERF), RTI International, and the University of Denver, is carrying out a research effort to assess and prioritize technology and related needs across the criminal justice community. This initiative is a component of the National Law Enforcement and Corrections Technology Center (NLECTC) System and is intended to support innovation within the criminal justice enterprise. For more information about the NLECTC Priority Criminal Justice Technology Needs Initiative, see www.rand.org/jie/justice-policy/projects/priority-criminal-justice-needs.

This report is one product of that effort. It presents the results of the Challenges with Digital Evidence Held in Remote Data Centers workshop, held in May 2017. The panel was convened to identify issues related to law enforcement acquisition of digital evidence held remotely. This report and the results it presents should be of interest to planners from law enforcement departments and courts, research and operational criminal justice agencies at the federal level, private-sector technology providers, and policymakers active in the criminal justice field.



This publication was made possible by Award Number 2013-MU-CX-K003, awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect those of the Department of Justice.

Limited Print and Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited. Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please visit www.rand.org/pubs/permissions.html. For more information on this publication, visit www.rand.org/t/RR2240.

© Copyright 2018 RAND Corporation

www.rand.org



The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND**® is a registered trademark.