JULY 2018

Low-Hanging Fruit

Evidence-Based Solutions to the Digital Evidence Challenge

Authors
William A. Carter
Jennifer C. Daskal

Contributor
William Crumpler

A Report of the CSIS Technology Policy Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

JULY 2018

Low-Hanging Fruit

Evidence-Based Solutions to the Digital Evidence Challenge

AUTHORS
William A. Carter
Jennifer C. Daskal

CONTRIBUTOR
William Crumpler

A Report of the CSIS Technology Policy Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

For over 50 years, the Center for Strategic and International Studies (CSIS) has worked to develop solutions to the world's greatest policy challenges. Today, CSIS scholars are providing strategic insights and bipartisan policy solutions to help decisionmakers chart a course toward a better world.

CSIS is a nonprofit organization headquartered in Washington, D.C. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look into the future and anticipate change.

Founded at the height of the Cold War by David M. Abshire and Admiral Arleigh Burke, CSIS was dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. Since 1962, CSIS has become one of the world's preeminent international institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global health and economic integration.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in November 2015. Former U.S. deputy secretary of defense John J. Hamre has served as the Center's president and chief executive officer since 2000.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Acknowledgments

We would like to thank the many people who have contributed to this report by participating in interviews and meetings and offering us feedback on the report and recommendations. In particular, we want to thank the representatives from federal, state, and local law enforcement and the Department of Justice who took the time to share their experiences and provided firsthand perspectives on the challenges of utilizing digital evidence in investigations and prosecutions. We also want to thank the representatives of technology companies who shared their insights into what service providers are currently doing to support law enforcement and what can be done to improve the relationship and facilitate enhanced cooperation. We are also grateful to the members of civil society organizations who helped to review our recommendations and identify opportunities to strengthen protections for privacy and civil liberties, while also strengthening law enforcement.

Finally, we especially want to thank David Bitkower, who not only offered his incredible wealth of expertise and experience, but also stepped up to help us to organize and conduct many of the interviews and discussions that informed our work. Without his help we would not have been able to reach such an incredible range of experts and leaders who were critical to this study.

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Contents

Executive Summary

The growth of digital technologies and the rise of mobile computing over the past decade have created new opportunities and new challenges for law enforcement. On one hand, the proliferation of digital communications, digital storage devices, and ubiquitous connectivity has made more information available than ever before on the movements, conversations, and behavior of people.

On the other hand, rapidly changing technologies, shifts in terms of who controls the data, adoption of sophisticated anonymity and obfuscation tools, and jurisdictional uncertainty create new and critical challenges for the detection, surveillance, and attribution of criminal activity. In fact, survey findings indicate that law enforcement officials across federal, state, and local entities encounter difficulties in effectively accessing, analyzing, and utilizing digital evidence in *over one-third* of their cases that involve digital evidence—a problem that is likely to grow over time absent national attention to this problem.

The purpose of this report is to focus attention on a range of too-often neglected challenges and opportunities faced by law enforcement as they seek to access and use digital evidence in their cases. Recently, most of the discussions have focused on encryption: to what extent, and in what circumstances, if any, should one be compelled to facilitate access to encrypted communications or otherwise inaccessible devices?[1] But the obstacles posed by encryption are just one aspect of the challenge in accessing digital evidence, albeit an important one. In many investigations, a range of data is potentially accessible to law enforcement pursuant to lawful means. For a variety of reasons, however, law enforcement officials often face significant obstacles in being able to access, decipher, or otherwise use that data, even when they have the legal authority to do so.

Our survey of federal, state, and local law enforcement officials suggests that challenges in accessing data from service providers—much of which is not encrypted—is *the biggest* problem that they

"... law enforcement officials across federal, state, and local entities encounter difficulties in effectively accessing, analyzing, and utilizing digital evidence in *over one-third* of their cases that involve digital evidence—a problem that is likely to grow over time absent national attention to this problem."

currently face in terms of their ability to use digital evidence in their cases. Specifically, the inability to effectively *identify* which service providers have access to relevant data was ranked as the number-one obstacle in being able to effectively use digital evidence in particular cases. Difficulties in *obtaining* sought-after data from these providers was ranked as a close second. These challenges ranked significantly higher than any other challenges—including challenges associated with accessing data from devices or interpreting the data that has been obtained.

This is an issue that has received relatively little attention and resources, and certainly not enough compared to the need. The sole federal entity with an explicit mission to facilitate more efficient cooperation between law enforcement and industry—the National Domestic Communications Assistance Center (NDCAC)—has a budget of $11.4 million, spread among several different programs designed to distribute knowledge about service providers policies and products, develop and share technical tools, and train law enforcement on new services and technologies, among other initiatives. Another important digital evidence training center—the National Computer Forensic Institute, run by the Secret Service—has to fight each year for adequate appropriations. This year it was awarded $18.9 million, enough for it to train approximately 1,200 students. If fully funded, it could train over 3,000 students per year.

An array of federal and state training centers, crime labs, and other efforts have been developed to help fill the gaps, but they are able to fill only a fraction of the need. Meanwhile, there is no central entity responsible for monitoring these efforts, taking stock of the demand, and filling the gaps. Nor is there any central entity responsible for the range of other, related policy concerns that have emerged and will undoubtedly continue to do so.

The good news is that these are problems that can be solved, or at the very least much better managed than they are now. This will require a national commitment, adequate resourcing, and a shift in policy. The costs are moderate and the payoffs likely large.

To fill these needs, this report calls for a new National Digital Evidence Policy, to be spearheaded by a National Digital Evidence Office that will have the responsibility for overseeing and coordinating the many efforts to fill the gaps. This office should, among other things, work with federal, state, and local law enforcement to track trends and challenges, and work with the other existing entities and individuals focused on these issues to improve law enforcement access to digital evidence, consistent with civil liberties. It should, for example, facilitate improved cooperation with service providers and help disseminate knowledge and analytical tools that can assist law enforcement in deciphering data that has been disclosed. And it should promote greater transparency about the nation's digital evidence policies and programs, ensure that new initiatives are being conducted in a manner consistent with privacy and civil liberties, and make recommendations with respect to new legal authorities and policy changes that are needed or being pursued.

The report further calls for the authorization and adequate resourcing of NDCAC or an equivalent entity to serve as a training and technical support center within this new office. Building on NDCAC's current mission, this support center would conduct and develop both in-person and online trainings; collect and disseminate knowledge about provider policies and products; educate law enforcement about how to submit lawful and appropriately tailored requests for data; develop and maintain technical tools for analyzing lawfully obtained digital evidence; and disseminate these tools to appropriately trained law enforcement personnel around the country.

Put simply, the current model—pursuant to which each and every office is largely expected to develop and maintain its own expertise—is not sustainable. Even with an extraordinary increase in funding and training,

it is not practical or possible for every one of the thousands of federal, state, and local law enforcement agencies across the country to have, within their own department, adequate access to all of the resources and expertise needed. In fact, more than half of those surveyed stated that they lacked sufficient internal resources to handle digital evidence—a problem that is likely to grow as more and more information becomes digitalized. It *is* possible, however, to effectively train agents and other relevant officials as to when expert advice or technical assistance is needed and where to go to seek it—so long as the training and expert assistance is widely available.

"... any workable solution will require renewed efforts by both law enforcement *and* the private companies that manage and hold data of interest."

In support of these efforts, the report also calls for the creation of an expert advisory board, comprised of experts from law enforcement, industry, and members of civil society, to advise the National Digital Evidence Office in a consultative role. This will facilitate better policies with broad multi-stakeholder support, foster the kinds of conversations and interactions needed to build trust (if not agreement) between parties, ensure a full range of perspectives are considered, and provide a venue for providers and other outside voices to raise concerns and/or push for policy changes.

Importantly, any workable solution will require renewed efforts by both law enforcement *and* the private companies that manage and hold data of interest. This report thus calls on tech companies that manage, store, and have access to data to do more as well. Specifically, the tech companies should commit to maintaining up-to-date law enforcement guidance, and better educating law enforcement on how their systems work and the kinds of data available, so as to avoid situations in which law enforcement has to guess what to ask for. This will in turn facilitate the submission of better and more tailored data requests from law enforcement, thereby eliminating a major source of concern on both sides of the process.

The report further calls on providers to maintain, and, if applicable, develop, online mechanisms through which law enforcement can make lawful requests for data; to commit to fast response times for emergency requests; and to ensure that there is a human being for law enforcement to speak with in the event of emergency. Providers should also commit to continued transparency about the nature and volume of requests, to challenge what they perceive to be overbroad or unlawful demands for data that they might receive, and to report trends of concern to the National Digital Evidence Office, via input to the expert advisory board or otherwise.

None of this is meant to replace the excellent work already underway in parts of the Department of Justice, across federal and district attorneys' offices, at federal and state crime labs, and in various other centers of excellence around the country. Nor is it meant to displace the efforts already underway by providers that have developed online portals to facilitate law enforcement access, make guides available to law enforcement, provide trainings, and engage in transparency reporting regarding law enforcement requests for data.

But both survey results and interviews suggest that there is more to be done. A National Digital Evidence Office would build on, elevate the prominence of, and ensure adequate resourcing for the successful initiatives already underway, and also help to ensure that training and technical assistance is provided not just to those that already receive it, but across the many federal, state, and local offices where the need arises.

Continued and increased engagement by tech companies would help ensure that law enforcement knows where to go to request particular data, the range of data available, and how to appropriately tailor their requests. Moreover, there is a clear need for best practices and industry standards that new entrants to the market and smaller-scale providers can adopt as well.

Some of these steps will take longer to achieve. It will, no doubt, take some time and effort to authorize and set up a new National Digital Evidence Office. But there are a number of steps that can and should be taken immediately. The Department of Justice can and should set up an internal national digital evidence coordinating body to fill the important policy and oversight needs. Congress can and should adequately resource NDCAC to serve the training and technical roles that already fall within its mission. The many excellent training centers that already exist should also be fully funded and should expand

their mission to reach a wider set of students and address a wider set of issues. Providers can and should also take voluntary steps to better facilitate access and tailored requests, consistent with the law and the need to protect privacy and civil liberties.

"These efforts are needed *no matter* the outcome of the separate debates around encryption and related issues."

The remainder of the report draws on survey results and a broad range of interviews to provide a detailed accounting and analysis of the four key areas of this report's focus: resource constraints, training programs, cooperation with service providers, and related legal and policy issues. Part II provides a detailed set of recommendations; part III provides conclusions.

What This Report Is *Not* About

Most of the discussions regarding law enforcement access to data have, to date, focused on things like encryption, lawful hacking and the vulnerability equity process, and other concerns related to the ephemerality of data and retention rules.[2] In fact, CSIS has a separate report on the encryption issue that we encourage all of you to read.[3]

The purpose of this report is to focus on the *other* obstacles to law enforcement access to data not covered in these discussions. These are issues of importance regardless of how one ultimately resolves the encryption debate, defines standards for lawful hacking, or addresses the data retention issue.

In focusing on this particular subset of issues, this report is not meant as a substitute for the ongoing debates and discussions on encryption, lawful hacking, and ephemerality—all of which will undoubtedly receive continued attention. But as highlighted in the pages that follow, there is much work that can and should be done to facilitate law enforcement access to data that is unencrypted or otherwise available in a way that is consistent with privacy and civil liberties, even as the policy discussions about potential decryption mandates, lawful hacking, and data retention continue.

There is a need for better coordination of the many training and support initiatives underway, improved exchange of information between service providers and law enforcement, and a national policy office dedicated to overseeing programming and needs, to taking steps to fill the gaps, to promoting better accountability and transparency, and to protecting privacy and civil liberties. These efforts are needed *no matter* the outcome of the separate debates around encryption and related issues.

Methodology

The report is based on extensive interviews with law enforcement officials, tech company representatives, and members of civil society, as well as a review of open-source material, budgets, training documents, and other source material regarding challenges faced by law enforcement in the field.

The authors conducted a series of off-the-record, closed interview sessions with dozens of federal, state and local law enforcement officials, representatives from major service providers, and representatives from civil society. These interviews provided a rich and textured analysis of the problems and range of possible solutions.

The report also draws on a nationwide survey carried out by the firm Vanson Bourne that targeted law enforcement officials from the federal, state, and local levels, across multiple jurisdictions, and multiple parts of the country. The survey provides a rich source of information regarding the challenges and needs of law enforcement entities across the country. Those findings are presented in the narrative that follows.

BACKGROUND

Our research identified and focused on four broad issues relevant to law enforcement's ability to effectively and appropriately leverage digital evidence: resource limitations, training needs, challenges involving cooperation with service providers, and a range of related legal and policy issues that have emerged.

On the resources side, effective use of digital evidence requires access to technical specialists, equipment, analytical tools, and legal expertise. But we found that these resources have not kept up with the growing importance of digital evidence to law enforcement's ability to effectively investigate and prosecute crime. Training programs have also failed to keep pace, both in providing a baseline level of digital evidence knowledge to all of law enforcement and the legal community, and in maintaining a pipeline of specialists to focus on specific challenges in dealing with digital evidence.

As more data is concentrated in the hands of service providers, the way in which law enforcement investigations are carried out has shifted. Increasingly, law enforcement does not conduct its own searches and seizures of evidence, but instead needs the assistance of these third-party providers to access the evidence and information it seeks. But the relationship between law enforcement and service providers has become strained, leading to a deep-seated distrust that makes effective and lawful cooperation more difficult than it should be. In fact, challenges that result from the interactions between law enforcement and service providers were defined as the number-one impediment to the effective use of digital evidence by law enforcement, according to our survey of law enforcement personnel.

All of this is happening against a backdrop of legal authorities from the pre-digital age that have been stretched and strained to maintain law enforcement's capabilities and protect civil liberties as technology rapidly evolves.

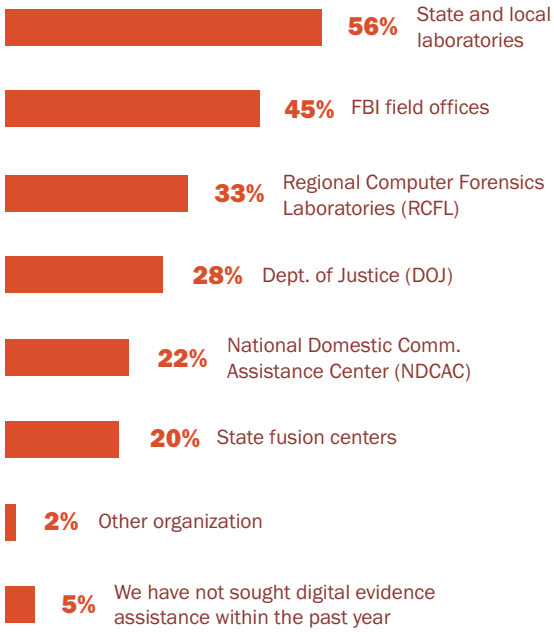
The following sections outline the key challenges in each of these areas that we identified in our research.

a. Resources

Accessing, analyzing, and utilizing digital evidence can require significant resources, including equipment to access data from devices, storage and computing power to manage large volumes of data, analytical tools to make sense of digital evidence, legal support to help prepare warrants, other forms of court orders, and subpoenas, and technical experts to handle data from a wide range of devices and platforms. While the importance of digital evidence to law enforcement has grown dramatically in recent decades, resources to address the problem have not kept pace.

According to our survey, only 58 percent of respondents felt their department has access to the resources, either internally or externally, needed to meet their digital evidence needs. The problems are particularly acute among local law enforcement. Just 45 percent of local law enforcement has, according to our survey, access to adequate digital evidence resources, whether within their own department or through larger state and federal departments and forensic labs. Federal entities, not surprisingly, fare much better.

Where Has Your Department Sought Outside Assistance with Digital Evidence in the Last 12 Months?



Yet, state and local entities—where most of the problems are concentrated—handle the vast majority of criminal investigations and prosecutions in the United States. Out of more than 3 million arrests for violent crimes in 2016, over 95 percent were carried out by state and local entities.[4]

Most departments and agencies do not have sufficient knowledge, facilities, or tools in-house. In fact, more than a third of small police departments surveyed have no forensic specialists on staff, and even larger departments and well-resourced agencies often have limited resources to meet their digital evidence needs internally. The New York County District Attorney's office, for example, is among the best-resourced local law enforcement entities in the country in terms of expenditures, tools, and people available to address digital evidence needs. Yet, even the New York DA's office has just 12 to 15 forensic specialists on staff to support 550 prosecutors handling over 100,000 cases a year.

As a result, departments often depend on state and federal laboratories, agencies, and other entities for digital evidence support. In fact, 95 percent of those surveyed sought digital evidence assistance in the past year, with state and local labs (56 percent) and FBI field offices (45 percent) getting the bulk of the assistance

ABOVE: CSIS survey of law enforcement professionals, conducted by Vanson Bourne between April and May 2018

requests. Regional Computer Forensics Labs (RCFLs), which are FBI-run centers that provide support with digital evidence collection, examination, and analysis, are a close third.

Resources Needed

As to be expected, the kind of assistance needed varies from case to case—ranging from identifying which service providers have access to relevant information, to obtaining and interpreting that data, accessing and interpreting evidence from devices, and using evidence in court. There are three broad categories of assistance needed: knowledge and expertise, lab facilities and equipment, and analytical tools to make sense of data that has been obtained. While, as noted above, law enforcement already has a range of resources available, these resources are insufficient to meet the need.

Knowledge and Expertise

Perhaps the most valuable resource for law enforcement is knowledge and expertise. Using digital evidence in investigations and prosecutions requires an understanding of what data is available; how to access it legally from hundreds of different devices, apps, operating systems, and service providers; what it means and how to use it; how to introduce it into court; and how to render it into a form that juries will understand.

Additional resources are needed to support education and training to grow this knowledge base. The need for additional education and training is discussed in more detail in the section that follows. However, even with much more extensive training, it is not feasible for everyone in the law enforcement community to share a detailed understanding of all of the digital devices and systems out there, how to access the data, and what to do with the data once it is obtained. Specialized repositories of expertise and skills are essential.

Some such repositories do exist, but none are sufficiently funded. And there is no single entity currently responsible for tracking the range of assistance programs available to law enforcement and/or directing agents to the appropriate sources of advice and assistance.

The National Domestic Communications Assistance Center (NDCAC), for example, is an FBI organization that focuses on supporting state and local law enforcement's efforts to get data from service providers. NDCAC maintains a website for its law enforcement customers with detailed information on the major providers' systems and how to submit digital evidence requests, as well as a hotline for law enforcement to call in for advice and support on dealing with providers. It is one of the key sources of knowledge and expertise. But NDCAC's budget is both small and divided among multiple different training and support programs—making it inadequately resourced to service the 18,000 federal, state, and local law enforcement entities spread across the country.

For legal guidance, many people turn to the Computer Crime and Intellectual Property Section (CCIPS) at the Department of Justice, whose staff advise law enforcement and prosecutors on preparing warrants, other kinds of court orders, and subpoenas. For CCIPS staff, however, this is another service provided on their own time alongside their main casework.

A range of other federal, state, and local entities has arisen to fill the gaps. The FBI's Computer Analysis Response Team (CART) has over 500 agents and hundreds of analysts and support staff across the FBI's 56 field offices and their headquarters in Quantico, Virginia.[5] Other federal agencies also provide some support, for example, the Drug Enforcement Administration's (DEA) Document and Media Exploitation Unit,[6] the U.S. Marshals Service's (USMS) Technical Operations Group (TOG),[7] and Immigration and Customs Enforcement's (ICE) computer forensics agents and digital forensics lab.[8] These units provide a range of support, including specialized technical skills needed to access data from a range of devices, assistance submitting evidence requests to providers, and analytical support to make sense of digital evidence.

State crime labs and major metropolitan police departments often serve as sources of knowledge, in addition to playing a key forensic role.

There are also nonprofits that maintain wikis, databases, how-to guides, and support lines for law enforcement. For example, the National Consortium for Justice Information and Statistics, an organization of states and territories that develops and disseminates information for law enforcement groups,

Many Different Resources

The following lists the range of federal, state, and local entities and offices that provide, in some form or another, digital evidence support. While many of these entities do excellent work, most are underfunded for their missions. And the need continues to outpace the supply.

ORGANIZATION	DESCRIPTION
State and Local Laboratories	State police agencies and major metropolitan police departments provide some digital evidence support to smaller local departments. For local police departments, state police agencies and FBI field offices are often the primary source of external digital evidence support.
FBI Field Offices	The FBI's Computer Analysis Response Team (CART) has agents and hundreds of support staff across the FBI's 56 field offices and their headquarters in Quantico, Virginia. In 2015, CART agents examined 37,600 pieces of media (9.77 petabytes) in support of 7,338 investigations. Agents from the FBI's Cyber Division also provide support and technical expertise to the broader law enforcement community.
Regional Computer Forensic Laboratories (RCFLs)	The FBI operates 18 Regional Computer Forensics Laboratories (RCFLs) across the United States, which provide digital forensics services to state, local, and federal law enforcement. RCFL staff conduct nearly 6,000 forensic examinations per year, and provide digital forensics training for state and local agencies. Each RCFL has about 15 staff—mostly detailed from the FBI and from state and local agencies—and offers a range of services from automated Cellebrite and Grayshift kiosks that extract evidence from mobile devices to full forensic examinations of seized devices.
Department of Justice (DoJ)	The DoJ offers legal and technical assistance to state and local law enforcement officials on the subject of digital evidence. Most prominently, the DoJ's Computer Crime and Intellectual Property Section (CCIPS) regularly provides guidance to law enforcement and prosecutors on how to prepare warrants and other legal process for acquiring digital evidence. Its digital investigative analysts have also been responsible for creating a number of analytical tools to help law enforcement agents parse the data they receive from service providers.
National Domestic Communications Assistance Center (NDCAC)	The FBI's National Domestic Communications Assistance Center (NDCAC) provides a wide range of digital evidence resources for state and local law enforcement, including maintaining an online guide to the major communications providers' platforms, developing parsing tools to help investigators make sense of data from service providers, and providing guidance on how to submit digital evidence requests to companies.
State Fusion Centers	Fusion centers are a network of 79 state- and local-run, federally supported organizations across the country dedicated to the analysis and sharing of information across state, local, and federal law enforcement organizations. Fusion centers provide training and technical assistance to local law enforcement, including with respect to digital evidence, although that is neither their sole nor primary mission.
Other Federal Agencies	Many federal law enforcement agencies also offer some digital evidence support services and training to state and local law enforcement: • One of the most highly regarded is the U.S. Secret Service's Cell Phone Forensic Facility in Tulsa, Oklahoma, which includes two Secret Service technical agents and also leverages faculty and students from the University of Tulsa's Cyber Corps Program to help law enforcement access data from locked smartphones. • The Secret Service also operates the Electronic Crime Special Agent Program, a group of over 1,400 Secret Service agents with the task of combating cyber threats to critical infrastructure. The agents are well-trained in digital evidence gathering and support digital evidence examination by state and local investigations. • The Drug Enforcement Agency (DEA) has a Document and Media Exploitation Unit (DOMEX) with 15 regional teams and 2 digital evidence labs that support major narcotics investigations. • The U.S. Marshals Service (USMS) has a Technical Operations Group (TOG) with about 100 personnel that provide surveillance and digital evidence support. • Immigration and Customs Enforcement (ICE) maintains a team of 315 computer forensics agents and operates a digital forensics laboratory.

runs SEARCH, which provides up-to-date information about service providers' policies and practices.

But while these entities and initiatives serve important functions, none are sufficient to meet the need—as is evidenced by survey results in which more than half of state and local law enforcement officials stated that they lacked sufficient resources to effectively handle digital evidence. Moreover, these efforts are uncoordinated and piecemeal. Some locations have lots of resources, some remarkably few. No single entity is currently responsible for assessing what's out there and what's needed and for taking the necessary steps to fill the unmet needs.

"No single entity is currently responsible for assessing what's out there and what's needed and for taking the necessary steps to fill the unmet needs."

Laboratories and Equipment

Using evidence from seized devices requires proper seizure and preservation, access to specialized equipment or lab facilities to conduct forensic exams, technically trained staff to figure out how to image data from devices and render it into a usable form, and the ability to translate that data into evidence that, if applicable, can be used in court. Whereas larger police departments often have evidence technicians and forensics specialists on staff to seize and process evidence, the cost of operating full-service crime labs and maintaining equipment is high. Key equipment like Cellebrite and Grayshift kiosks to extract data from mobile phones can cost tens of thousands of dollars.[9]

These are things that few state and local police departments can afford. They instead rely on crime labs operated by large departments and agencies. A 2014 survey by the Department of Justice identified 409 publicly funded crime labs in the United States, of which 79 offered dedicated digital evidence support services. This includes 18 Regional Computer Forensics Laboratories run by the FBI, as well as crime labs run by state law enforcement agencies and major metropolitan police departments.[10]

The following map shows the distribution of federal and state crime labs that offer broad-scale digital evidence services across the country. It does not include local labs, although some, particularly the major urban police departments and attorney general offices, such as in New York and Los Angeles, provide forensic services to smaller police departments in their areas. As is evident, many of the resources are concentrated on the seaboards and in major urban areas. There are large areas, particularly in the western states, but also in places such as Ohio and West Virginia, with no nearby facilities—meaning that agents have to travel far distances if they seek the kind of assistance that cannot generally be provided remotely, such as accessing data from devices.

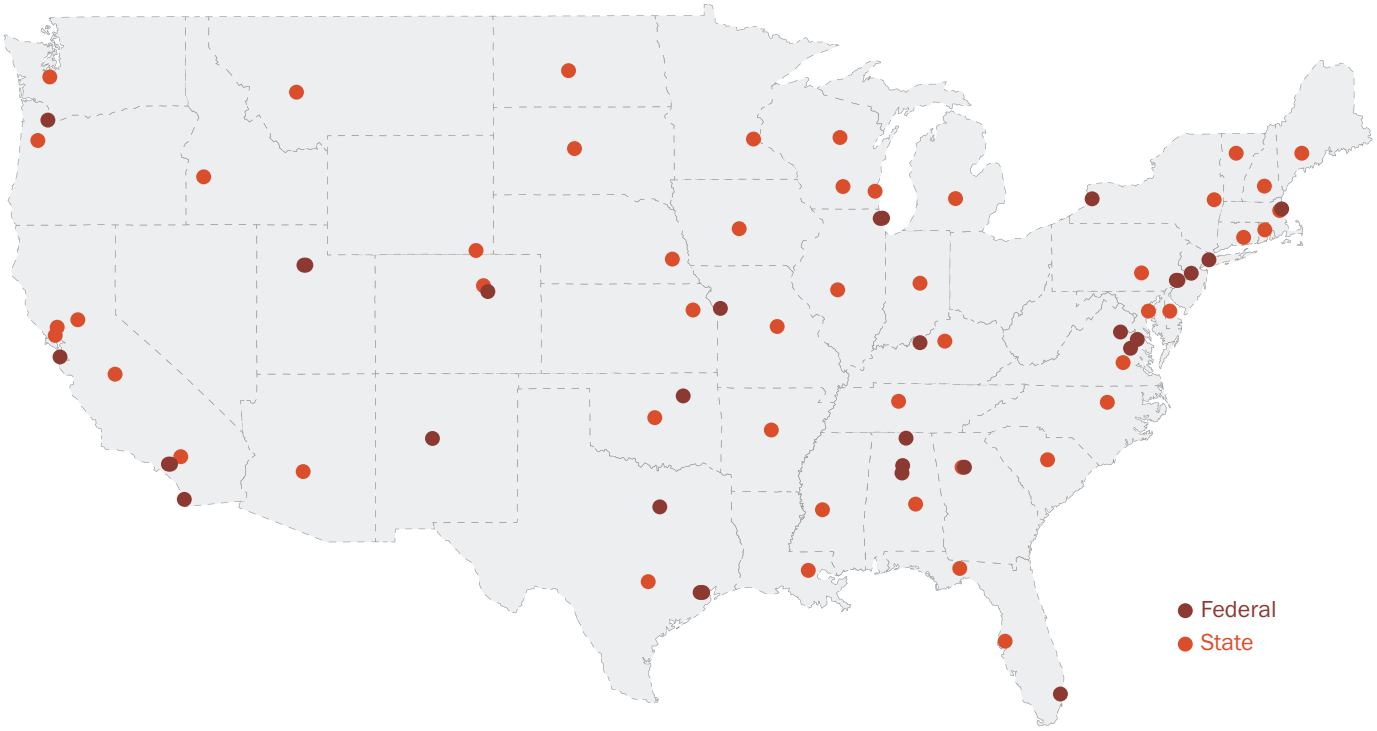
Analytical Tools

Even when data has been lawfully disclosed, and law enforcement is clearly entitled to such data, it can be incredibly challenging for law enforcement to interpret the data. Some providers will, for example, send law enforcement large files with long strings of unpunctuated, unseparated characters that need to be parsed into distinct words, phrases, and messages. Doing so requires access to analytical tools that can help decipher what is otherwise perceived as incomprehensible. In other cases, the data returned by service providers is provided in encrypted form along with a decryption key; this requires the ability to use the decryption key so as to render the data readable.

There are a few different agencies that develop and maintain these tools for law enforcement, but dedicated funding to develop or acquire tools is rare. NDCAC currently maintains eight parsing tools to help law enforcement make sense of returns from service providers, but has to balance this role with its training and technical and legal case support functions—all on a very tight budget.[12] CCIPS has developed some tools to help law enforcement and prosecutors make sense of data disclosed by service providers. But again, this is a side service for CCIPS staff, who already have busy day jobs.

Some vendors also offer analytical tools for law enforcement, but they are generally quite expensive. Interviews also suggest that they these kinds of off-the-shelf tools are increasingly ineffective. Providers are, after all, constantly upgrading and adapting their systems. As a result, the off-the-shelf tools are not only costly, they are often not up to the task.

Federal and State Digital Evidence Laboratories Across the United States



Need Continues to Outstrip Supply

Use of digital evidence in investigations and prosecutions is challenging. It requires an understanding of what data is available, how to access it legally from hundreds of different devices, apps, operating systems, and service providers, what it means and how to use it, and how to render it into a form that juries will understand. There are, to be sure, a number of resources and groups that provide advice and expertise on an ad hoc basis, many of which do exemplary work. But even just figuring out where to find this investigative, legal and technical expertise is an enormous challenge for investigators and prosecutors.

Even the FBI, whose Science and Technology branch has an annual budget of $600–800 million and over 6,000 staff,[13] struggles to meet its own digital evidence needs. The Operational Technology Division (OTD) houses some of the most sophisticated capabilities in the law enforcement community, but according to many law enforcement officials it can be difficult to leverage their capabilities in criminal cases. Moreover, priority is given to national security cases.

The limited resources available are stretched thin across the nearly 18,000 law enforcement organizations in the United States. The NDCAC, for example, is meant to be the go-to resource for state and local law enforcement, but has an extremely limited budget given its mission and the need. While federal and state crime labs provide a range of services, there are only a few available in each state, and accessing their equipment can mean a drive of hundreds of miles for some investigators.

One senior official from the International Association of the Chiefs of Police (IACP) estimated that demand for digital evidence support from state and federal agencies exceeds available resources by at least 50 percent.[14] He also suggested that the real need is probably much greater, given that the challenges many investigators face just to submit requests for assistance are so high that many do not even request the support they need. Both the survey results and interviews with a range of federal, state, and local prosecutors and investigators support that estimate and suggest it may even be higher.

ABOVE: Map includes federal and state crime labs listed in the 2014 Bureau of Justice Statistics (BJS) survey of publicly funded crime laboratories and the International Association of Chiefs of Police (IACP) directory of cybercrime labs. It does not include local and municipal crime labs, although some of those, especially at major urban police departments and attorney general offices, provide digital evidence services to smaller police departments in their areas.[11]

b. Training

Knowledge of digital systems and how to access, handle, and utilize digital evidence is increasingly important to virtually every type of criminal case, but dedicated training in evidence handling, recovery, analysis, and storage is limited. To be effective in the digital age, investigators and prosecutors have to understand what data is available, which devices or providers can be used to access to it, how it can be analyzed and used in investigations, and what process is required to lawfully access the data and use it in court. Those surveyed, however, reported that they got an average of just 12 hours of digital evidence training in the last year, and almost half receive training just once every two years or less.

Average Number of Hours of Digital Evidence Training in the Last 12 Months

Local 10 hours

State 13 hours

Federal 16 hours

Judges, too, need to know enough information to be able to issue appropriately tailored warrants and court orders, address issues such as evidence handling, treatment of irrelevant data, and privacy interests of affected third parties, and respond to legal challenges. Adequate training of judges—although not captured in the survey, which focused exclusively on law enforcement personnel—is of critical importance as well.

There are, to be sure, a number of training programs available to law enforcement for different types of digital evidence. But while many are excellent, they are generally under-resourced and not sufficient to meet the need.

ABOVE: CSIS survey of law enforcement professionals, conducted by Vanson Bourne between April and May 2018.

Most of the best training programs are based on a model of bringing students to centralized training centers, which allows for in-depth, concentrated training, but has a high cost per student and requires those being trained to take a full week away from the other parts of their jobs. This makes sense for those being trained as specialists. But it is an inefficient means of teaching the full range of law enforcement entities the basic information—things like evidence preservation and where to go for additional assistance when needed—that every officer needs to know.

Moreover, there is no central entity overseeing and coordinating the various training efforts and taking steps to identify gaps and fill needs. Currently, for example, a significant portion of existing training programs targeting law enforcement officials focus on accessing data from seized devices. Identifying and accessing data from service providers, in contrast, is less likely to be the central focus of digital evidence trainings, despite its growing importance for investigations across the country.

Existing Digital Evidence Training Programs for Law Enforcement

The nation's largest provider of law enforcement training is the Department of Homeland Security's Federal Law Enforcement Training Center (FLETC). FLETC provides a range of training and certification programs for specialists including Digital Evidence Acquisition Specialists and Digital Evidence Analysts.[15] These programs are by all accounts well run, but they cost thousands of dollars per student and focus primarily on seized devices.[16]

Another highly regarded program is the Secret Service's National Computer Forensics Institute (NCFI) in Huntsville, Alabama. The NCFI provides week-long, in-depth courses on how to access, handle,

and analyze digital evidence, and serves a combination of law enforcement officials, prosecutors, and judges. It, too, operates on a model of bringing students to Huntsville, and is currently operating well below capacity due to budget constraints. With its current budget of $18.9 million, the NCFI is running at about one-third capacity, training 1,200 state and local law enforcement officers per year. NCFI has developed a five-year growth plan to expand; at full capacity, it would cost approximately $35 million and serve over 3,000 students a year.

NDCAC is one of the only providers of digital evidence training that focuses largely on training law enforcement officials on identifying which service providers have access to relevant information and how to access that data. Yet, the NDCAC's annual budget is just $11.4 million, divided between its training, tool development, and hotline services.[17] Moreover, its current training model also requires students to travel to its training center. This costs about $50,000 per class for about 50 students, meaning it can train just 1,800 students a year. NDCAC is currently working to develop training modules that it can bring directly to the students—rather than requiring students to come to its center. This is a worthwhile initiative that should be adequately resourced and pursued.

State entities also provide training opportunities. The Massachusetts Attorney General's Office, for example, has for the past six years run a National Cyber Crime Conference that provides hundreds of individual training sessions run by police, prosecutors, forensic experts, and judges over a course of three days. At relatively low cost, and with a wide menu of different training opportunities to choose from, it attracts participants from all across the country and has trained thousands of law enforcement officials over the past six years.[18]

Other training opportunities are provided by private companies and nonprofits. For example, companies like the Public Agency Training Council (PATC) and Police Technical offer a range of digital evidence and computer crime training courses for law enforcement, as do nonprofits like the National Consortium for Justice and Statistics and the National White Collar Crime Center (NW3C).

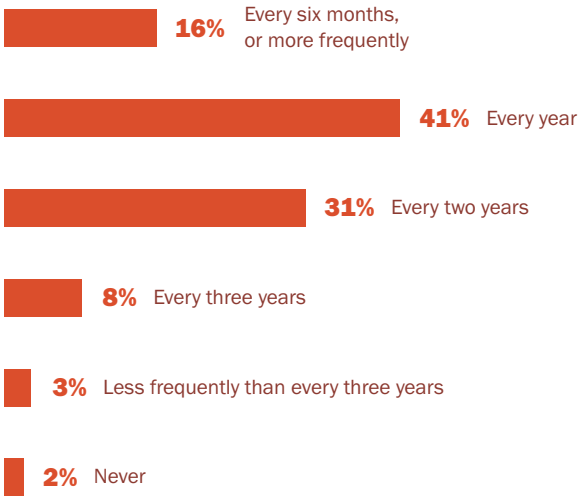
Gaps Remain

As already stated, one of the biggest challenges is that the training centers operate as specialized centers where law enforcement, prosecutors, and judges come to be trained as digital evidence specialists. For state and local law enforcement across the country, accessing training programs at places like the NCFI or NW3C can require traveling thousands of miles and missing more than a week of work. The cost of facilities, travel, and time away from the office make it more difficult for law enforcement to get regular training to maintain their skills and knowledge of the digital environment.

ABOVE: elen31/ Adobe Stock

How often do you receive digital evidence training?

Total combined percentages from local, state, and federal law enforcement



LEFT: CSIS survey of law enforcement professionals, conducted by Vanson Bourne between April and May 2018.

Some organizations, including NDCAC and many of the major service providers, have begun offering traveling courses where trainers are sent out to regions across the country to provide local training opportunities to law enforcement in those areas. Other organizations should look to replicate this model wherever possible to ensure that state and local law enforcement have access to these programs.

"Every officer and agent is expected to have a basic knowledge of how to collect, preserve, and utilize fingerprints and DNA as evidence. But every officer is not expected to be able to analyze or interpret the evidence—that is the job of specialists and specialized labs. The same should be true of digital evidence."

Training challenges are made even more difficult by turnover and changes of assignments. An investigator who develops an understanding of how to use email data in white-collar crime investigations may be reassigned to auto theft, or may leave for a lucrative job in the private sector. This leaves the base of knowledge across the law enforcement community far too shallow.

Addressing these challenges requires a five-pronged approach. *First*, the reality is that just about every agent is going to encounter digital evidence. All law enforcement should be trained in the basic understanding of how to properly preserve evidence, the kind of information likely available on seized devices, and the resources available to lawfully access and interpret relevant data. This should be incorporated into basic training for all officers.

Second, increased efforts should be spent on building up digital evidence expertise in offices across the country. This means that specialized training programs with demonstrated success like NDCAC and NCFI that focus on digital evidence should be expanded significantly. As just one example, the NCFI's budget should be increased to $35 million so that it can scale up to full capacity, training over 3,000 individuals per year, as compared to about 1,200 individuals now. These organizations should also invest in expanding their regional training programs to ensure that they can reach a wider audience across a bigger segment of the country.

Third, a recognition that even with increased training and skill development, not every agent can be a forensic specialist. And not every department will have sufficient expertise to assist all of its investigators and prosecutors. As a result, there is a continued need to build up and expand centralized repositories of expertise, such as state crime labs and federal centers like NDCAC, which can provide expert assistance to entities across the country.

An analogy can be made to fingerprints and DNA. These evidentiary tools have become ubiquitous in investigations. Every officer and agent is expected to have a basic knowledge of how to collect, preserve, and utilize fingerprints and DNA as evidence. But every officer is not expected to be able to analyze or interpret the evidence—that is the job of specialists and specialized labs. The same should be true of digital evidence.

Fourth, resources should be invested in training judges, in addition to law enforcement officials engaged in the investigative and prosecutorial functions. Judges serve as crucial intermediaries in the request process, ensuring that data requests are lawful and appropriately tailored. Resources should also be expended to train defense attorneys, who also need the ability to access and interpret digital evidence in order to mount an adequate defense.

Fifth and finally, a systematic review of the training programs and curricula available to law enforcement, attorneys, and judges must be undertaken. This review should locate gaps and inconsistencies in training, and identify which programs are and are not effective in meeting law enforcement's needs. For example, many of the existing programs focused on digital evidence for law enforcement focus on data from devices, while training for requesting and utilizing data from service providers is more limited. The results of this review should be used to fill gaps in existing programming and, where appropriate and effective, standardize curricula and training practices.

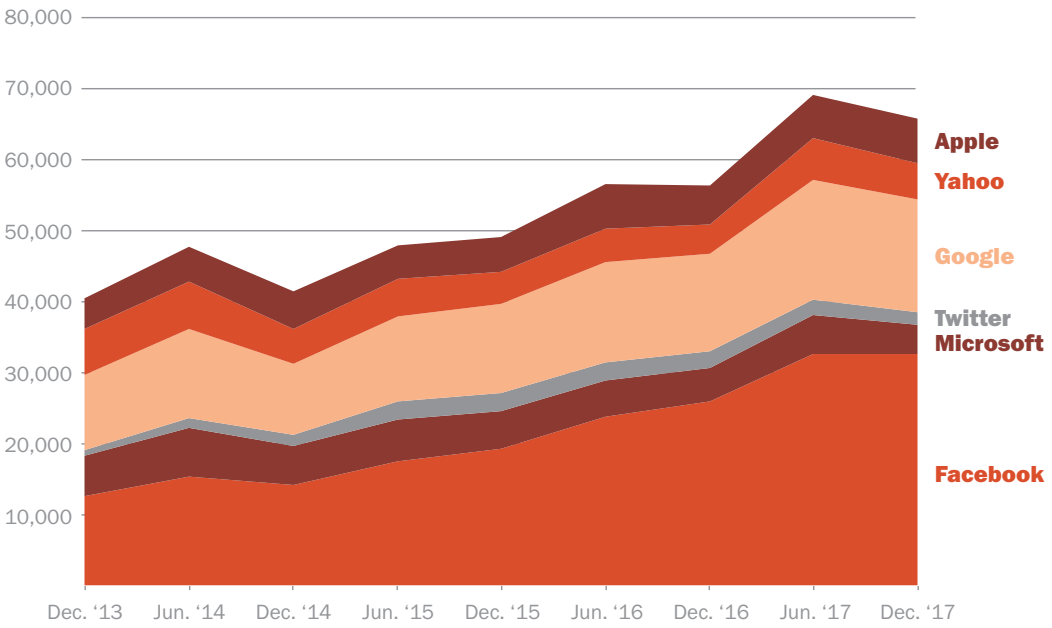
c. Cooperation with Service Providers[19]

Over the past decade, there has been a sea change in how investigations are carried out. Prior to the rise of digital communications, law enforcement officials would only infrequently need the assistance of third-party providers to access sought-after evidence; most of it was in the hands (or homes) of the investigative targets themselves. Now increasingly law enforcement needs the assistance of third-party companies to carry out their investigations.

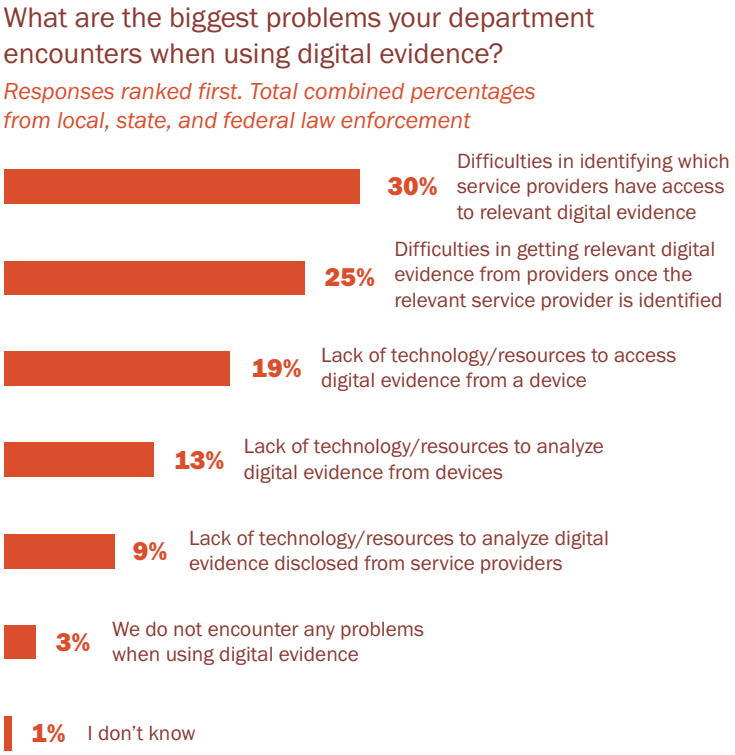
In 2017, U.S. law enforcement made over 130,000 requests for digital evidence to just six tech companies—Google, Facebook, Microsoft, Twitter, Oath (formerly Yahoo!), and Apple—with Facebook and Google getting the bulk of these requests. Add in Verizon, AT&T, and Comcast and the numbers jump to over two-thirds of a million. These requests covered everything from communications content to metadata (such as location information) and names and IP addresses of particular users.

These numbers only cover a portion of the interest. They only include the requests actually made—not those never initiated because law enforcement didn't know where to go to seek data or how to make the requests. They also only cover the largest tech

U.S. Law Enforcement Data Requests to Major Technology Companies



LEFT: Transparency reports for Facebook, Microsoft, Twitter, Google, Yahoo, and Apple.[20]



companies. As everything from driving routes to sleep patterns to home entry comes to be digitally recorded by connected devices, the so-called "internet of things" (IoT), a growing amount of information collected by smaller IoT companies is likely to become of interest to law enforcement as well.

The increased digitalization of society presents both opportunities and challenges. In many cases, it means that law enforcement is able to access a lot more information a lot more efficiently, and without risking tipping off the target of the investigation. (This is particularly true given the prevalence of no-notice orders, which also preclude the provider from telling its customer of the fact that his or her data has been requested.)

But it also creates significant challenges for law enforcement. Effective use of digital evidence presents a dizzying array of choices and issues for law enforcement: What services does the investigative target use? What information does that service provider have? What is the appropriate and lawful means for requesting and/or compelling disclosure from that provider? How does one make sense of the data that is eventually returned to law enforcement? And how can it be effectively introduced and authenticated in court?

In fact, identifying which service providers have access to relevant digital evidence was ranked as the *biggest* challenge in dealing with digital evidence across federal, state, and local law enforcement officials. Notably, law enforcement perceived that much of the sought-after data is out there in the hands of service providers, but just not available or easily accessible to them for a range of reasons. Survey results thus ranked problems identifying what data exists and which service provider had access to it as significantly bigger challenges than lack of data in the hands of service providers.

The challenges of obtaining and using data from service providers also ranked higher than challenges associated with accessing and interpreting data found on devices.

Credibility Gap

Our interviews indicated a deep credibility gap on the part of both law enforcement and service providers that significantly undercut the ability of both sides to work with one another to facilitate lawful and legitimate access to data.

Law enforcement officials expressed deep frustration at what they perceive as slow response times and the inability to talk to an actual human being on the provider side who can help them work through any issues with requests, despite the fact that, in their view, many of the major technology companies could readily afford to expend additional resources on their law enforcement teams. They reported a concern that requests were being turned down if they did not use the right "magic words," meaning providers expected law enforcement to refer to their data by the same terms that they did, even though law enforcement officials pointed out that they lack the detailed knowledge of providers' systems to know exactly what data they hold and how they label it.

▲ *ABOVE: CSIS survey of law enforcement professionals, conducted by Vanson Bourne between April and May 2018.*

Law enforcement officials also suggested that some providers are deliberately seeking to forestall lawful access, including in the ways that they design their systems. They expressed concern that providers were failing to disclose the extent of available information—which could in turn be critical to effectively investigating and prosecuting crime. And they expressed frustration at receiving data in what appears to be unwieldy or unstructured formats, and suggested that it would be relatively simple for providers to share data with law enforcement in intuitive formats. In particular, law enforcement expressed concern that data was being made available to advertisers and other business customers that was not shared with them.

Providers, for their part, described deep-seated frustration with what they viewed as overbroad and boilerplate requests from law enforcement. They argued that law enforcement does not appreciate their dual responsibility to provide lawful access to data for law enforcement and protect their users' privacy.

They emphasized that the mere fact that law enforcement officials seek access to particular data doesn't necessarily mean that the request is appropriate and lawful, or that the data is even available. There are, after all, situations in which sought-after data is simply unavailable, or there is reasonable disagreement over what kinds of information can and should be lawfully obtained. In particular, providers complained that they were often issued broad-based requests for data that were not, in their view, appropriately tailored.

Providers also pushed back on many of the critiques from law enforcement. They described significant efforts spent to train law enforcement, develop law enforcement guidance, and ensure that law enforcement could lawfully access data. They asserted that they work diligently to respond to requests, and suggested that time delays were often caused by law enforcement, not them. One particular source of delay relates to questions over user notification. Most companies' policy is to disclose law enforcement requests to the subject of the relevant request, unless the request is accompanied by a non-disclosure order precluding such information sharing. But they recognize that this can be disruptive to investigations and therefore also sometimes check with law enforcement before doing so—often waiting weeks or more for law enforcement to decide whether or not to obtain the order.

In some ways, the data supports both narratives. The *number* of law enforcement requests, at least as directed at the major U.S.-based tech and telecom companies, has significantly increased over time. Yet, the *response rates* have been remarkably consistent. As a result, law enforcement is having more requests turned down in terms of actual numbers. But the *percentage* of cases in which major third-party providers are pushing back remains relatively steady (hovering around the 20 percent range), at least according to self-reporting by major providers.

These numbers, however, only capture the number of requests made—the number doesn't address those requests never made because law enforcement doesn't know where to go to make the request or decides not to make it because similar requests have been rejected or responded to in ways that make them unhelpful in the past. And both qualitative and quantitative research indicates that there are also a range of situations in which there is available data relevant to an ongoing investigation that can be lawfully obtained—and yet law enforcement is stymied in being able to access that data because of lack of clarity as to where to direct the request, how to make the request, and/or how to decipher data that has been lawfully disclosed.

Moving Forward

Fixing this requires effort—and additional resources—on the part of *both* law enforcement and the providers.

Specifically, law enforcement can and should do more to educate themselves about providers' policies and practices; to appropriately tailor requests to providers; to ensure that online requests for data are appropriately authenticated; and to develop, maintain, and distribute tools to interpret data that has been obtained. These are things that many law enforcement entities are already doing, many in an exemplary way. But the need for training and distribution of knowledge continues to outpace the supply. This requires policy coordination, enhanced resources, and engagement by Congress.

That said, these efforts will be effective only if there is sufficient information made available to law en-

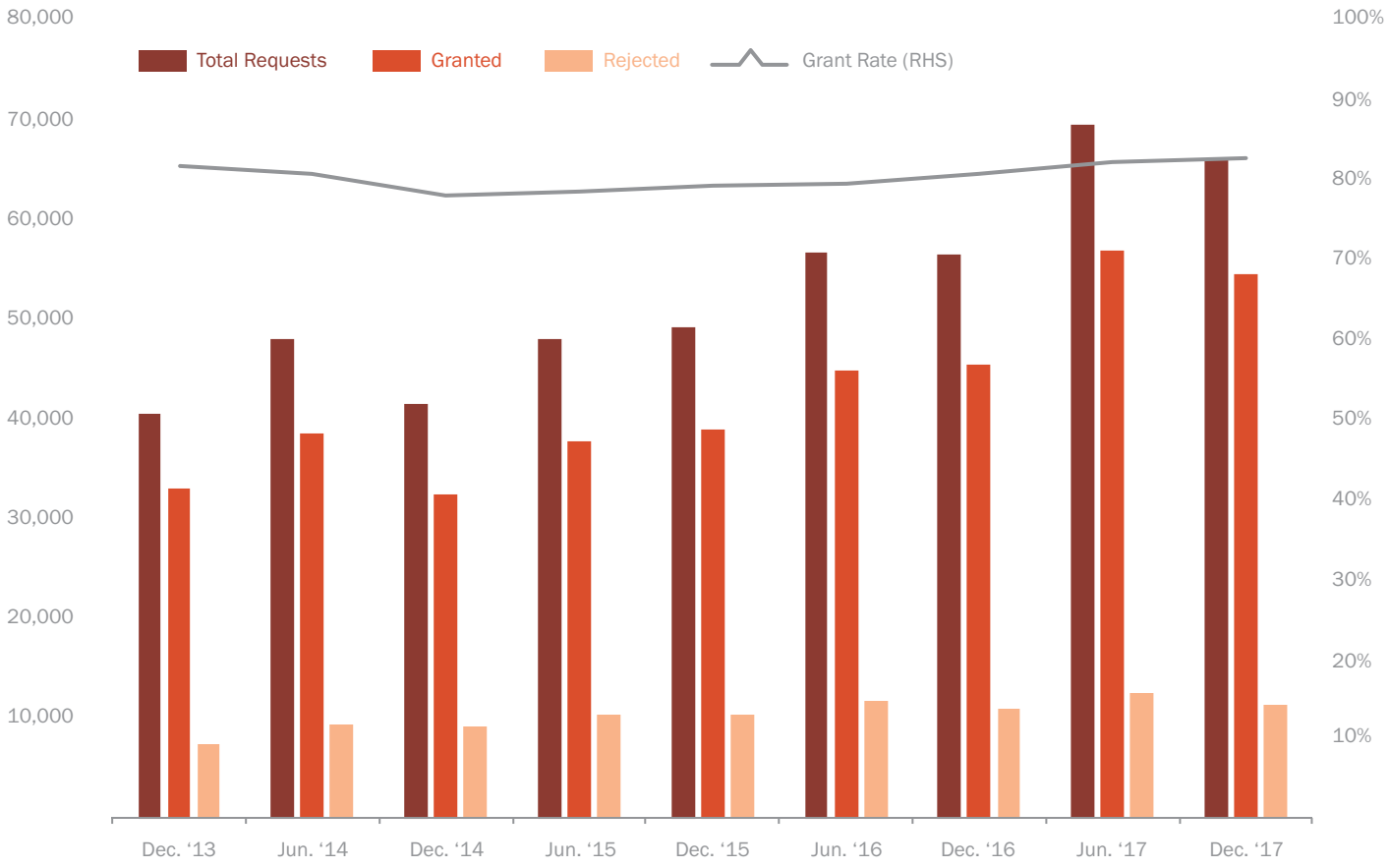
forcement. Providers can and should do more to ensure that this is the case. Providers should do more to inform law enforcement of the kinds of data that is available, adequately resource their law enforcement compliance teams, communicate about the reasons that requests are rejected, and ensure there are up-to-date and efficient tools for law enforcement to make online requests for data. These, too, are things that many of the major tech companies are already doing. By further investing in these efforts, providers will help ensure that law enforcement has the tools and knowledge they need to make appropriate and tailored requests.

BELOW: Transparency reports for Facebook, Microsoft, Twitter, Google, Yahoo, and Apple. Full bibliographic information included in reference section.

"Fixing this requires effort—and additional resources—on the part of *both* law enforcement and the providers."

These are also all issues that many smaller providers have not yet focused on. These issues should be considered and incorporated into business plans and counsel jobs, as they will inevitably find themselves subject to an increasing number of law enforcement requests for data over time.

U.S. Law Enforcement Data Requests Submitted to US Tech Companies



d. Additional Legal and Policy Issues

There are a range of different legal authorities that come into play and are relevant to the ability of law enforcement to access digital evidence. As an overarching matter, there are four key federal statutory authorities governing access to digital evidence: the Stored Communications Act[21]; the Wiretap Act[22]; the Pen Register and Trap and Trace (Pen/Trap) Act[23]; and the Communications Assistance for Law Enforcement Act (CALEA).[24] Demands for digital evidence are in many cases also governed by the Fourth Amendment. Meanwhile, state law provides additional requirements and protections in certain instances as well.[25]

Arguably the most important statute for accessing digital evidence by law enforcement is Title II of the Electronic Communications Privacy Act of 1986 (ECPA), also known as the Stored Communications Act (SCA), which regulates the disclosure of stored communications data. To access a target's stored communications, such as emails or instant messages, from a provider's servers requires a warrant under a combination of the SCA and Fourth Amendment doctrine.[26] Pursuant to the recent Supreme Court ruling in *Carpenter v. U.S.*, warrants are also now required for certain kinds of historical location data; the ruling may also lead to warrants being required for a wider range of digital evidence previously available by other forms of court order or subpoena, although the full implications of the ruling remain unclear.[27]

Other communications data, for example, metadata and subscriber information, can be accessed via a form of court order less rigorous than a warrant, or by subpoena.

The SCA was amended in March 2018 to, among other things, clarify that warrants issued pursuant to the SCA require service providers to disclose all responsive data in their custody or control, regardless of where the underlying 0s and 1s are located.[28] This was a direct response to pending litigation in what was known as the *Microsoft Ireland* case, in which the Second Circuit had ruled that SCA warrants only reached data physically located within the territorial boundaries of the United States—a result that was making it difficult for U.S. law enforcement to access sought-after data based on the happenstance of where a third-party provider decided to store it.[29] There are other, ongoing efforts to update the SCA—which was enacted in 1986, before there was anything akin to the modern internet. These efforts are the subject of much ongoing discussion and debate—a debate likely to intensify in the future.

Our focus here is on some additional legal and policy challenges that have largely been overlooked—and that survey and interview results suggest are needed. Specifically, we identify four key areas of focus: the authentication of digital evidence in court; the authentication of law enforcement's identities when making requests; security and privacy issues associated with evidence that has been collected; and tailoring of legal requests for data. We conclude by noting some of the many other unresolved legal and policy issues that have arisen and will continue to arise, the need for a dedicated office designed to think through and address these issues, and the need for international cooperation and consultation.

Authentication of Digital Evidence to Be Used in Court

Traditionally, authentication of digital evidence has required a custodian of the evidence to testify as to how the data was generated and the underlying systems relied on to access the data. This can be incredibly costly and burdensome. For law enforcement, it means the expense of bringing in someone to testify for just a few moments about chain of custody. For providers, it means that members of law enforcement compliance teams are spending their days in court hearings rather than doing other things of import, like responding to law enforcement requests for data.

Reforms to the Federal Rules of Evidence went into effect on December 1, 2017, which respond to this problem on the federal side. The rules now explicitly provide for the self-authentication of digital evidence if appropriately certified, meaning that service providers do not have to send their legal and technical experts to testify to the authenticity of evidence and can instead work on responding to other requests.[30]

Many of the state systems, however, have not caught up. This is a particular problem in New York, where the scope of what can be self-authenticated is quite limited. Prosecutors must call a live witness from each service provider to authenticate emails, photos, and other communications content, even if the particular evidence would otherwise be subject to an exception to the hearsay rule.[31] This is costly and burdensome—requiring the expenditure of unnecessary travel costs and time.

This should be changed—something that the New York White Collar Task Force and a range of tech companies and others have already urged.[32] Other states should make the necessary reforms as well so as to ensure electronic evidence can, in appropriate cases and in ways that continue to permit challenges based on confrontation rights, be authenticated via certification.

Authentication of Requesting Law Enforcement Identity

The use of online portals and other online data request mechanisms raises questions about how to verify the identity of the requester and thereby protect against unauthorized disclosures of data. As the volume of online requests increases, it may become increasingly difficult for companies to determine who is and is not a legitimate law enforcement officer submitting a legally valid request. Without some mechanism to verify that a requester is truly a member of law enforcement working a legitimate case, there is a risk that data will be disclosed to inappropriate individuals. The process of

Other Important Surveillance and Digital Evidence Statutes

CALEA

▶ **In 1994**, Congress passed the Communications Assistance for Law Enforcement Act (CALEA), amending the Wiretap Act to help law enforcement to conduct lawful wiretaps. Under CALEA, common carriers, facilities-based broadband Internet access providers, and providers of interconnected Voice over Internet Protocol (VoIP) service (defined to be "telecommunications carriers" under CALEA) are required to ensure that their systems are capable of isolating and enabling the interception of specified communications content and records in response to lawful process.

No similar requirement applies with respect to internet communications, including emails and over-the-top applications, such as WhatsApp and use of social media accounts. The SCA also does not carry any reporting or accountability requirements, despite the sensitivity of the vast amounts of data collected under SCA warrants.

Pen Register Trap and Trace Statute

▶ **Applications** for pen registers and trap and trace devices under the Pen/Trap Act, which track incoming numbers dialed or received from a phone, require an application under oath that the information is "relevant" to an ongoing criminal investigation. They can be authorized for renewable periods of 60 days. Notice is precluded unless authorized by the court.

reviewing and responding to requests by providers will be slowed as they attempt to verify the origins of requests.

This is a difficult problem to solve. But currently there is no entity focused on even identifying the various options, let alone developing an authentication system that can be put in place. The federal government should take this on, ideally in partnership with the providers, state, and local authorities. It should start by identifying the various options—perhaps looking at how the FBI verifies the credentials of those law enforcement agents seeking access to its various fingerprint and other available databases as a start. The goal should be to develop a system that can be shared with all federal, state, and local law enforcement entities and the providers, so as to help ensure that providers are disclosing customer data to those with authority to request it.

Minimization, Security and Transparency

The key statute dealing with access to digital evidence from service providers—the SCA—says nothing about how to deal with the handling of information collected, nor does it include any reporting or oversight requirements. This is in contrast with the rules governing wiretaps, which impose stringent minimization procedures on law enforcement, requiring them to put in place a mechanism to avoid the collection of information on third parties not subject to the order, and to provide detailed annual reports on all Title III wiretaps to Congress.[33] These requirements were put in place because the data collected from wiretaps was viewed as highly personal and sensitive, but the data available from smartphones and online platforms today can provide a much more comprehensive and intrusive view of a person's life and habits than a phone call. The rise of the internet of things, and consequent exponential growth of precise data on every aspect of our daily lives, will only exacerbate this challenge.

The absence of any rule or regulations governing the data collected also is in contrast with foreign intelligence authorities, which also require, as a matter of statute, the adoption of minimization rules designed to limit the acquisition, retention, and dissemination of information concerning non-consenting U.S. persons (defined to include U.S. citizens and residents) in the course of acquiring data of otherwise authorized targets of foreign intelligence surveillance.[34]

This is something that can and should be addressed. It is, after all, almost inevitable that even the use of targeted warrants will yield incidental collection on persons with whom the target of the investigation has communicated. Some of this may be relevant to the investigation, some not. There is thus a need to

The Wiretap Act

Intercepting data in real time falls under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III, also known as the Wiretap Act). Wiretaps, which allow for live interception of communications content, are authorized only with respect to certain types of criminal investigations, although that list has grown significantly over the years to cover a wide range of such investigations.[35]

The process for obtaining a wiretap is more stringent than for stored communications content. The judge issuing the warrant must determine, among other things, that there is probable cause to believe that the particular communications obtained will be about the crime being investigated and that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous."[36]

Title III also mandates that the Administrative Office of the United States Courts provide detailed annual reports to Congress on the use of Title III wiretaps. These reports include, among other things, details of wiretap applications and approvals, the underlying crimes being investigated, the number of communications intercepted, and the number of targets affected, as well as whether the taps resulted in prosecutions and convictions.[37]

LEFT: CHANDAN KHANNA/AFP/Getty Images

think through rules and best practices with respect to the retention and dissemination of third-party data as well as the security of the data being held.

"Put simply, unless law enforcement officials are adequately informed about what kind of data providers have available, they are not in a position to know what there is to ask for—let alone determine if it is relevant."

Moreover, even with respect to data of targets themselves, issues regarding the retention, dissemination, and security of collected data are not things that have been adequately considered or addressed to date. At the most basic level, there is a need to adequately protect the security of the data from hackers and other nefarious actors. There is also a need for practices and procedures regarding how long collected data can be retained, who it can be shared with, and for what purposes.

We do not here propose any specific resolution of the issues. But they are critical to consider—particularly as the use of digital evidence grows over time. A National Digital Policy Office would be uniquely situated to evaluate the competing interests and concerns and help craft an appropriate set of policies and rules to take into account the intersecting security and privacy interests at stake.

Scope of Requests

Law enforcement must meet different standards depending on the kind of evidence being sought. For stored content and certain cell-site location data, providers must obtain a warrant, based on a finding that there is probable cause to believe that the information is evidence of a crime that has been or is being committed. The warrant standard also requires what is known as particularity—requiring that the warrant "particularly describe" the evidence to be searched or seized. For court orders under the SCA, the government must present "specific and articulable facts showing that there are reasonable grounds to believe" that the evidence is "relevant and material to an ongoing criminal investigation." Subpoenas require only relevance.

The level of specificity required under law thus varies based on the kind of information sought and the particular instrument used to compel production. But in all cases there is a requirement that the evidence sought be relevant—and in many cases much more.

Specificity on the part of law enforcement can also help improve coordination between law enforcement and service providers. The more tailored the request, the less burden there is on providers and, as a result, the more likely that the provider is able and willing to comply.

But a requirement of specificity creates a problem for law enforcement, who may not know in advance what information providers have that may be relevant to their investigation—or what language to use to request that data in ways that will elicit a provider response (what law enforcement described above as the "magic words" problem). To deal with this uncertainty, law enforcement frequently asks for, in addition to specifically identified information, the catch-call category of "any and all relevant data."

Providers sometimes balk at such requests, particularly in those situations when they are not subject to additional time or other scope limitations. As several providers emphasized, the demand for "any and all" data is burdensome and, if not appropriately tailored, unduly places the obligation on them to determine what is and is not relevant—something that they are generally not equipped to do given that they only have access to limited facts about the underlying case.

Law enforcement claims, conversely, that they often lack enough information to know what data is and is not available and make the kind of relevancy deter-

mination needed. Put simply, unless law enforcement officials are adequately informed about what kind of data providers have available, they are not in a position to know what there is to ask for—let alone determine if it is relevant. Law enforcement officials also point out that in many cases it is appropriate to ask for "any and all data," particularly when the universe of available data is sufficiently limited—for example, if the request is directed toward "any and all data" about a particular account and during a specific time horizon.

Both parties need to do more to address this problem. Providers should be more candid about and better educate law enforcement about their products and services so as to enable law enforcement to make more appropriately tailored requests. Law enforcement, conversely, should take steps to avail themselves of available information offered by providers, for example ensuring that they review law enforcement guidance issued by companies before submitting requests, and avoid catch-all requests for "any and all" data without additional specificity. Judges too should demand this in the issuance of warrants and other court orders.

But this, of course, requires that the law enforcement guide be comprehensive about the available sources of evidence—and that, equally importantly, law enforcement trusts that the information provided is comprehensive. We highlight the importance of both comprehensive law enforcement guidance and provider participation in training of law enforcement in the recommendations below.

Novel Issues

The use of digital evidence by law enforcement raises—and will continue to raise—a host of novel legal and policy issues, separate from the encryption issues that dominate the current discussions, all of which touch on multiple different equities and require careful consideration and thought. What, if any, limitations should be placed on law enforcement's ability to comb through—or rely on private entities to comb through—social media to generate individual profiles on individuals and predict risk? What standard of proof should be required to access the range of data made accessible by the internet of things? What are the appropriate rules governing biometric data? How should pre-internet laws be interpreted to cover these issues? What, if any new laws, policies, and procedures are needed? The recent Supreme Court decision in *Carpenter* only exacerbates the challenges—leaving open and therefore ripe for litigation a range of unresolved questions about whether and to what extent the Fourth Amendment protects different types of data disclosed to third-party providers.

"There should be a dedicated office within the Department of Justice focused on these issues and with the resources and mandate to identify and address the full range of equities at stake."

These are issues that individuals and offices scattered throughout the federal and state governments are considering. But there is no central entity tasked with thinking through the many legal, policy, and ethical issues that arise—and will continue to arise in the future. Given the critical importance of each and every one of these issues to security, privacy, and the economy, this should change. There should be a dedicated office within the Department of Justice focused on these issues and with the resources and mandate to identify and address the full range of equities at stake.

International Coordination

While this report focuses on the needs of the U.S. law enforcement community, the challenges facing law enforcement in its ability to access digital evidence are high on the agenda of other countries as well. The European Commission, for example, recently put forward a Draft Regulation and Directive designed to address law enforcement challenges in accessing digital evidence—much of which is, akin to this project, designed to facilitate the relationship between law enforcement and service providers.[38]

Meanwhile, Interpol is initiating a range of training programs and seeking to disseminate technical skills in a manner similar to what NDCAC is seeking to do.[39]

A National Digital Evidence Office could and should work with international partners to build synergies, foster a common approach, and promote international developments consistent with both security needs and respect for privacy and civil liberties.

RECOMMENDATIONS

The following recommendations respond to the findings in the report. As stated from the outset, the focus is on the range of issues that limit law enforcement access to digital evidence, separate from issues associated with encryption, ephemerality, and the use of lawful hacking. These recommendations are by no means meant to be a substitute for ongoing debate around those critically important areas. But regardless of whether or how the encryption debate is resolved, and regardless of the rules developed with respect to lawful hacking, there will continue to be a need for better cooperation with service providers, more trainings, and increased resources devoted to accessing data that is available. These recommendations focus on those issues.

As an overarching measure, the report recommends the creation of a National Digital Evidence Office to play the key coordinating and policy role needed, and for adequate resourcing of the training programs and dissemination of technical expertise and other relevant knowledge needed. To be clear, a National Digital Evidence Office is not in any way meant to displace the excellent work being done within the Department of Justice, the FBI, and among the various other federal, state, and local entities providing expertise, analytical tools, and trainings. Instead, it will provide a central repository of information about the programs available, help to identify gaps in resources and training, direct resources to the areas of greater need, and engage in the kind of policy oversight and coordination needed. All of this, we hope and expect, will help to ensure that these issues are given the national attention that they deserve.

It also calls on providers to do more to educate law enforcement about their products and policies, to provide an explanation of the reasons why requests are rejected, and to thereby help ensure the issuance of appropriate and tailored requests for data.

The following elaborates on all of these recommendations and provides key details. And while some of these recommendations require congressional authorization and appropriation, many others can be implemented immediately without congressional action. We urge all relevant parties to do what they can to take immediate action to fill some of the identified needs, even as we simultaneously urge Congress to take up the mantle and both authorize the institutions and provide the training needed.

To Congress

Authorize and provide adequate resources to a National Digital Evidence Office to engage in the following overarching tasks: serve as a central unit to, in coordination with existing efforts underway, assess and respond to law enforcement's digital evidence needs; establish a national digital evidence policy; stay up to date with changing technologies and trends; and update policies in response to changing technologies and trends, if and when appropriate; all in accordance with a mission of protecting privacy and civil liberties.

The specific mission of the office shall include the following:

Identify and Rectify Gaps: Conduct relevant research and analysis to identify the biggest challenges with respect to law enforcement's ability to access and analyze digital evidence. Identify and respond to training effectiveness and gaps.

Coordinate Grantmaking: Work with the Office of Justice Programs (OJP) and other grantmaking bodies to support law enforcement access to digital evidence, including support for training programs, development and distribution of analytical tools, and maintenance of crime labs. Grantmaking should be contingent on compliance with national digital evidence policy, reporting requirements, established best practices, and the full range of commitments directed at law enforcement below.

Data Management and Security: Establish and promote the use of a consistent set of clear standards for securing and minimizing data collected by law enforcement.

Authentication System: Work with providers and law enforcement entities from across the federal, state, and local systems to identify options for, and ultimately develop, a system for verifying that a person requesting data from a service provider is in fact a law enforcement official entitled to access it.

Coordinate with International Efforts: Work with international partners to build synergies, help set baseline standards and practices that promote both security and civil liberties, and, to the extent practical and helpful, harmonize efforts across borders.

Report to Congress/Accountability: Provide annual reports to Congress about ongoing activities, including but not limited to information about: grant recipients; ongoing efforts to identify and respond to gaps in training and distribution of technical tools; the state of cooperation with providers; novel uses of legal authorities; and any new policies and best practices being seriously considered or that have been adopted. This report shall be made publicly available. If necessary, it can be coupled with a non-public annex addressing sealed requests for data or other sensitive information about ongoing cases.

Authorize and provide adequate resources to the National Domestic Communications Assistance Center (NDCAC), as a support center within the National Digital Evidence Office, to serve as a central clearinghouse for training, provision of technical expertise, and legal assistance for criminal investigations. The mission of the center shall include the following:

Dissemination of knowledge/cooperation with providers: Serve as centralized repository of knowledge and expertise about provider systems and procedures for submitting requests for data.

Production and dissemination of technical tools: Build and maintain analytic and forensic tools to assist law enforcement in interpreting data that has been obtained from service providers and devices, employing technical specialists that can help develop and maintain those tools.

Provide training: Provide trainings at the federal, state, and local level, leveraging preexisting entities (such as state and regional computer forensics labs and training facilities) to distribute knowledge and expertise. Produce and maintain training materials and curricula for use by other training organizations and departments. Coordinate with efforts already underway at Europol, federal and state training programs, and existing private-sector and nonprofit initiatives. Partner with providers on training initiatives for law enforcement officials, prosecutors and judges, and defense attorneys.

Hotline Services: Provide a 24/7 hotline for law enforcement officials to seek advice about accessing and analyzing digital evidence in their cases.

Adequately resource other effective training programs, such as the National Computer Forensic Institute (NCFI), National While Collar Crime Center (NWC3), and others to train law enforcement, prosecutors, and judges on the use of digital evidence.

Authorize and fund a dedicated federal grant program to be managed by OJP and the National Digital Evidence Office that will consolidate already-existing grant programs designed to facilitate law enforcement access to data and use those resources to fund state and local law enforcement agencies to provide training and to acquire and disseminate equipment and tools to process and analyze digital evidence, consistent with the priorities established by the National Digital Evidence Office. Tie grant issuance to demonstrated success and to adherence to key commitments directed at law enforcement below.

Authorize and mandate a Digital Evidence Expert Advisory Board, comprised of representatives from law enforcement, industry, and members of civil society. This board will provide input to the National Digital Evidence Office on trends, challenges, and proposed policy changes. The board will also be available to respond to issues and questions that arise.

- To promote transparency and encourage broader public input, the board should be required to hold at least one public meeting a year. It should also be exempted from Federal Advisory Committee Act requirements that it make all meetings open to the public—requirements that will inhibit the kind of open, frank discussions needed for this board to effectively fulfill its mission.

Provide a mechanism, via a combination of public meetings or an online portal, for members of the public to raise complaints and concerns.

To Federal/State/Local Law Enforcement Authorities

- Provide adequate and appropriate training on digital evidence requests to all necessary personnel, including incorporating training on digital evidence requests into basic training and taking advantage of the wide range of national and local training centers, online tools, and specialized training offered by organizations like NCFI, NDCAC, NW3C and others.
- Provide continuing education for law enforcement personnel on relevant technology and communications platforms, including how to submit appropriately tailored requests for digital evidence, consistent with existing legal requirements and protections for privacy and civil liberties.
- Review providers' law enforcement guidance and other available materials related to the types of data law enforcement seeks before submitting requests.
- Make requests as specific as possible to facilitate rapid and full response by providers, and tailor boilerplate search warrants to the needs of specific cases.
- Keep up-to-date records of the number of devices obtained and accessed. Report challenges in accessing and analyzing data from providers or devices to the National Digital Evidence Office.

To Judges

- Ensure that warrants and court orders are appropriately tailored and specific.
- Hire and/or consult with technical experts on issues associated with law enforcement requests for digital evidence.
- Take advantage of opportunities for continuing education for judges on lawful access to digital evidence, changes in technology, and the challenges that emerge.

To Providers

- Provide regular trainings to law enforcement entities at the federal, state, and local level on what information is potentially available and on company policies in order to facilitate tailored and specific requests from law enforcement.
- Maintain up-to-date and comprehensive law enforcement guidance and make it available online.
- Develop and/or maintain online mechanisms to receive law enforcement requests for data and to provide dated, electronic confirmation of receipt of the request.
- Provide a sufficiently detailed explanation of the reason for rejecting a request for data in whole or substantial part, so as to enable law enforcement to understand the basis for denial and make revisions or seek judicial remedy, if necessary.
- Commit to rapid response times. For providers that are frequent recipients of law enforcement lawful requests for data, respond or make a human being available to speak to as rapidly as possible, and in all cases within six hours in cases of emergency involving danger of death or serious physical injury to any person.[40]
- Ensure appropriate staffing and resources to handle law enforcement requests for data and conduct regular evaluations of compliance needs.
- Report details about the volume and nature of law enforcement requests for data. Include in existing transparency reports general reasons for rejecting the requests (i.e., data not available, lack of legal authority). Break down, where possible, the authority being relied on (warrant, other court order, or subpoena) and the nature of the data being sought (i.e., content, non-content, location data).
- Commit to challenging any unlawful requests and to reporting trends of concern to the National Digital Evidence Office and National Digital Evidence Advisory Board.
- Leverage experiences, knowledge, and resources of larger providers to assist smaller providers, including, for example, those managing interconnected devices and a range of different apps, in setting up mechanisms for dealing with law enforcement requests for data and the legal requirements that apply.

"... the more is invested, the greater the impact on law enforcement's ability to access the data they need."

Costs

Some of these efforts can be done at relatively low cost, requiring relatively few offsets, particularly if done creatively by, for example, detailing existing governmental employees to these new positions, utilizing existing office space, and consolidating grant programs that already exist. That said, the more resources provided to the office to, for example, hire additional technical experts and conduct trainings across the country, and to fund grant programs that can support state and local efforts, the more effective the office and the policy will likely be.

In our view, minimum costs would include the following: (i) Hiring of a minimum of 10 to 15 technical experts to build up NDCAC's forensics team; help maintain and distribute up-to-date tools for interpreting data disclosed by providers; and work to develop effective authentication tools for online requests for data. (ii) Hiring of 10 to 15 additional staff to support NDCAC's goals of developing and disseminating training materials, working with providers, and making staff available 24/7 to assist with emergency requests for data. (iii) Hiring of a director, deputy director, and administrative assistant to run the National Digital Policy Office. (iv) Hiring of a part-time administrative assistant/part-time staff to help set up the Advisory Committee, organize the logistics, and assist with information gathering and policy development. Additional staff could be detailed from other agencies and sections of the Department of Justice.

Additional expenditures could include more staff and attorneys for both the policy office and NDCAC; travel costs for both staff and the Advisory Board; office equipment and supplies; and any honorarium paid to Advisory Board members. Providing adequate staff to both the policy office and NDCAC will be essential to meet the growing needs of law enforcement across the country.

Providing additional funding to grant programs to state and local law enforcement is also important. In particular, the effectiveness of new programs for state and local departments, and the ability to hold them to high standards of oversight and accountability, will be proportional to investment.

We estimate that these needs can be met with an expenditure of as little as $10 million or less for the key staff and support costs to $100 million or more depending on how these efforts are staffed and how much money is allocated for new grant programs. As mentioned above, the more is invested, the greater the impact on law enforcement's ability to access the data they need.

CONCLUSION

Digital evidence will only grow in importance as more of our lives move online and connected devices proliferate. As the world changes, law enforcement's capabilities and authorities will need to evolve to keep up, and the relationship between law enforcement and major service providers will become ever more essential to protect the rule of law and public safety, as well as privacy and civil liberties. Regardless of the outcome of ongoing debates around issues like encryption, data retention, and lawful hacking, additional resources, training opportunities, and improved coordination mechanisms between law enforcement and service providers will be necessary to meet this growing need.

Many excellent programs and initiatives are already underway at federal, state, and local law enforcement agencies across the country, providing expertise and guidance, access to lab facilities and technical skills, and legal advice to under-resourced departments and agencies. Meanwhile, major providers are also working to address the challenges created by increased law enforcement demands for evidence by, among other things, operating online portals to facilitate data requests, developing law enforcement guidance, and issuing transparency reports to help keep the public informed.

But despite these ongoing efforts, the status quo is not sustainable. Law enforcement faces significant problems in identifying which providers have what information and thus obtaining needed data, even when there is a clear need for the data and a legal basis to access it. Limited resources and disparities in how resources are distributed leave many offices without the tools and resources they need to effectively access and analyze critical information. The range of challenges is only likely to grow as more of our lives become digitized and as the government, courts, private parties, and ordinary citizens continue to struggle with foundational questions about the appropriate scope of governmental access to digital evidence and the substantive and procedural rules that should apply.

A National Digital Evidence Policy is needed, one that can address and respond to new trends in technology. Establishing a national office within the Department of Justice will help raise the profile of the issues and ensure they are given the kind of focused attention that they need. Such an office is uniquely situated to build on and coordinate the excellent work of others at the federal, state, and local levels, take a holistic, strategic view of the resources available, assess and respond to the gaps that exist, and play a proactive role in directing funding streams and setting policy going forward. The housing of technical experts and others that directly assist state and local entities with their cases—via the placement of NDCAC—within this office will build synergies and further help to ensure that policies are developed with a clear understanding of the technical challenges and specific needs.

Congressional action to authorize and fund this new office and new programs is needed. But there is also much that can be done with existing resources and authorities in the interim. Providers can and should take steps to facilitate the effective and lawful sharing of information by, for example, doing more to educate law enforcement about the kinds of data available, explaining why requests are denied, and committing to rapid response times. The law enforcement community can do more to educate themselves about service providers' practices and seek outside assistance when they are not sure about where to go or how to ask for specific kinds of data. Following NDCAC's recent initiatives, training programs can and should focus more on regional and local trainings—bringing the trainers to the law enforcement officials and thus cutting down on costs. And judges too should play a more proactive role in ensuring that warrants and court orders are appropriately tailored and in seeking the assistance of technical expert if appropriate and necessary. These are all steps that can be taken immediately, even before Congress takes the additional actions that are needed.

As technology evolves, new challenges will continue to arise. Difficult debates about encryption, data retention, and lawful hacking will continue, as they must. But there is a need and an opportunity to address many of the other challenges facing law enforcement in its effective and lawful use of digital evidence, regardless of how these debates are resolved. A strategic approach that improves coordination, increases resources, raises the profile of the issues, and can evolve over time will improve law enforcement's ability to protect the public, and also strengthen privacy and civil liberties.

About the Authors

William A. Carter is deputy director of the Technology Policy Program at CSIS. His research focuses on international cyber and technology policy issues, including artificial intelligence, surveillance and privacy, data localization, cyber conflict and deterrence, financial sector cybersecurity, and law enforcement and technology, including encryption. He has spoken at events and conferences around the world and participated in Track 2 dialogues on cyber and technology policy issues with China, Russia, and Australia. Before joining CSIS, he worked in the Goldman Sachs Investment Strategy Group, where he performed research and analysis on geopolitics and the macro economy. He previously worked at the Council on Foreign Relations and at Caxton Associates, a New York hedge fund. He graduated from New York University with a B.A. in economics.

Jennifer C. Daskal is a senior associate in the CSIS Technology Policy Program and an associate professor of law at American University Washington College of Law, where she teaches and writes in the fields of criminal, national security, and constitutional law. From 2009–2011, Daskal was counsel to the assistant attorney general for national security at the Department of Justice (DOJ). Prior to joining DOJ, Daskal was senior counterterrorism counsel at Human Rights Watch, worked as a staff attorney for the Public Defender Service for the District of Columbia, and clerked for the Honorable Jed S. Rakoff. She also spent two years as a national security law fellow and adjunct professor at Georgetown Law Center. From 2016–2017, she was an Open Society Institute Fellow working on issues related to privacy and law enforcement access to data across borders.

Daskal is a graduate of Brown University, Harvard Law School, and Cambridge University, where she was a Marshall Scholar. Recent publications include Borders and Bits (*Vanderbilt Law Review* 2018); Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues *(Journal of National Security Law and Policy* 2016); and The Un-Territoriality of Data (*Yale Law Journal* 2015). Daskal has published op-eds in the New York Times, Washington Post, and International Herald Tribune and has appeared on BBC, C-Span, MSNBC, and NPR, among other media outlets. She is an executive editor of and regular contributor to the Just Security blog.

William Crumpler is a research assistant with the Technology Policy Program at CSIS, where his research focuses on cybersecurity policy and the governance of emerging technologies. He holds a B.S. in materials science and engineering from North Carolina State University.

Endnotes

1 See, for example, National Academies of Sciences, Engineering, and Medicine, *Decrypting the Encryption Debate: A Framework for Decision Makers* (Washington, DC: The National Academies Press, February 2018). https://doi.org/10.17226/25010; James A. Lewis, Denise E. Zheng, and William A. Carter, *The Effect of Encryption on Lawful Access to Communications and Data* (Washington, DC: CSIS, February 2017), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170221_Lewis_EncryptionsEffect_Web.pdf?HQT76OwM4itFrLElok6kZajkd5a.r.rE; Andreas Kuehn and Bruce McConnell, "Encryption Policy in Democratic Regimes: Finding Convergent Paths and Balanced Solutions," EastWest Institute, February 15, 2018, https://www.eastwest.ngo/sites/default/files/ewi-encryption-us-version.pdf.

2 There are some exceptions. See, for example, Sean E. Goodison, 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, CA: RAND Corporation, 2015), https://www.rand.org/pubs/research_reports/RR890.html;

3 Lewis, Zheng, and Carter, *The Effect of Encryption*.

4 Federal Bureau of Investigation, "Crime in the U.S. 2016," Uniform Crime Reporting Program, 2016, https://ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016.

5 PEAKE, "Customer Spotlight: FBI Computer Analysis Response Team (CART)," http://peake.com/resource-center/blog/customer-spotlight-fbi-computer-analysis-response-team-cart/.

6 U.S. Department of Justice, "Drug Enforcement Administration FY 2018 Performance Budget Congressional Submission," https://www.justice.gov/file/968916/download.

7 U.S. Department of Justice, "United States Marshals Service FY 2018 Performance Budget," https://www.justice.gov/file/968956/download.

8 U.S. Department of Homeland Security, "U.S. Immigration and Customs Enforcement Budget Overview," https://www.dhs.gov/sites/default/files/publications/CFO/17_0524_U.S._Immigration_and_Customs_Enforcement.pdf.

9 Digital Shield, "Products," https://digitalshield.net/products.

10 Matthew R. Durose, Andrea M. Burch, Kelly Walsh, and Emily Tiry, "Publicly Funded Forensic Crime Laboratories: Resources and Services, 2014," U.S. Department of Justice Bureau of Justice Statistics, November 2016, https://www.bjs.gov/content/pub/pdf/pffclrs14.pdf.

11 Ibid.; International Association of Chiefs of Police, "Directory of Cybercrime Labs – Area of Expertise = digital evidence and forensics lab," http://www.iacpcybercenter.org/resources-2/regional-labs-and-agencies-search/#; Regional Computer Forensics Laboratory Program Office, "Service Areas," https://www.rcfl.gov/service-areas.

12 National Domestic Communications Assistance Center, "Executive Advisory Board Meeting Minutes," May 17, 2017, https://ndcac.fbi.gov/file-repository/may2017eabmeetingminutesappendices.pdf/view.

13 Ellen Nakashima, "Meet the woman in charge of the FBI's most controversial high-tech tools," *Washington Post*, December 8, 2015, https://www.washingtonpost.com/world/national-security/meet-the-woman-in-charge-of-the-fbis-most-contentious-high-tech-tools/2015/12/08/15adb35e-9860-11e5-8917-653b65c809eb_story.html?noredirect=on&utm_term=.1298d9129803.

14 Personal interview (not for attribution – notes on file with authors), October 20, 2017.

15 Federal Law Enforcement Training Centers, "Impact Report Fiscal Year 2014," 2014, https://www.fletc.gov/fletc-impact-report-2014.

16 Ibid.

17 National Domestic Communications Assistance Center, "Executive Advisory Board Meeting Minutes," May 17, 2017, https://ndcac.fbi.gov/file-repository/may2017eabmeetingminutesappendices.pdf/view.

18 National Cyber Crime Conference, "Event Summary," 2018, http://www.cvent.com/events/2018-national-cyber-crime-conference/event-summary-c23534b8311048eab9ce451f53f7763f.aspx.

19 We use this term broadly to refer to any private entity that handles and controls digital evidence of interest to law enforcement. This includes, for example, device manufacturers like Apple, platform developers like Facebook, providers of internet services like Google, and providers of apps and digitally connected devices.

20 Facebook, "Government Requests for User Data," https://transparency.facebook.com/government-data-requests; Microsoft, "Law Enforcement Requests Report," https://www.microsoft.com/en-us/about/corporate-responsibility/lerr/; Twitter, "Information Requests," https://transparency.twitter.com/en/information-requests.html; Google, "Requests for User Information," https://transparencyreport.google.com/user-data/overview?hl=en; Oath, "Government Data Requests," https://transparency.oath.com/reports/government-data-requests.html; Oath, "Prior Reports," https://transparency.oath.com/prior-reports.html; Apple, "Report History," https://www.apple.com/privacy/transparency-reports/.

21 18 U.S.C. 2701 et seq.

22 18 U.S.C. 2511 et seq.

23 18 U.S.C. 3121 et seq.

24 47 USC 1001 et seq.

25 See, for example, California Electronic Communications Privacy Act, Ca. Penal Code § 1546, et seq.

26 While the statute itself specifies that certain communications content (held for 180 days or more or held by a remote communications service) can be obtained by court orders and subpoenas that fall short of the requirements of a warrant, the Sixth Circuit has concluded that as a matter of Fourth Amendment law, access to emails requires a warrant. Longstanding efforts at Electronic Communications Privacy Act (ECPA) reform have sought to make that ruling applicable to all communications

content and codify it as part of the Stored Communications Act (SCA); this is something that should be taken up by Congress and enacted.

27 *Carpenter v. United State*s, 585 U.S. __ (2018).

28 Clarifying Lawful Overseas Use of Data (CLOUD) Act, H.R. 1625, 115th Cong. div. V (2018) (enacted) (to be codified in scattered sections of 18 U.S.C.).

29 See Jennifer Daskal, *Microsoft Ireland*, the CLOUD Act, and International Law Making 2.0, https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/

30 See Fed. Rules of Evidence 902(13)-(14).

31 District Attorneys Association of the State of New York, "Report of the New York State White Collar Crime Task Force," September 2013, https://www.manhattanda.org/wp-content/uploads/2018/02/WCTF-Report.pdf at 18.

32 Ibid.

33 See 18 U.S.C. 2518-2519.

34 See, for example, 50 USC 1801(h); 1805(3); 1825(e).

35 The list of so-called predicate acts is at 18 USC Sec. 2516(1).

36 18 U.S.C. 2518 (3)(c).

37 18 U.S.C. 2519 (3); "Wiretap Report 2017," U.S. Courts, December 31, 2017, http://www.uscourts.gov/statistics-reports/wiretap-report-2017.

38 European Commission, "E-evidence – cross-border access to electronic evidence," April 17, 2018, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

39 INTERPOL, "Activities—Capacity building," https://www.interpol.int/Crime-areas/Cybercrime/Activities/Capacity-building; INTERPOL, "INTERPOL launches first digital forensics training course for wildlife investigations," June 30, 2017, https://www.interpol.int/News-and-media/News/2017/N2017-086.

40 Six hours tracks what has been proposed as the standard in the European Commission. In many cases, emergencies will require even faster response times. A recent Washington attorney general report, for example, indicates that law enforcement has an average of one hour in a child abduction case to locate the perpetrator and victim before the child is murdered. See Katherine M. Brown, Robert D. Keppel, Joseph G. Weis, and Marvin E. Skeen, "Case Management for Missing Children Homicide Investigation," Office of the Attorney General of Washington and the U.S. Department of Justice Office of Juvenile Justice and Delinquency Prevention, May 2006, https://www.atg.wa.gov/child-abduction-murder-research.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | www.csis.org