A HOOVER INSTITUTION ESSAY

Small Towns, Big Companies: How Surveillance Intermediaries Affect Small and Midsize Law Enforcement Agencies

ANNE E. BOUSTEAD

Aegis Series Paper No. 1802

As the commercial collection of information about consumers has become ubiquitous, the scope of information that law enforcement can obtain from commercial entities has boomed. Although government access to commercially collected information about individuals can provide crucial evidence for criminal investigations and counterterrorism efforts, it can also pose serious risks to individual privacy. Consequently, policy-makers and scholars have paid significant attention to how law, technology, and commercial practices mediate law enforcement access to commercially collected information. In the legal domain, this debate has centered around efforts to interpret the Fourth Amendment in light of changes in consumer technology, especially as it relates to the third party doctrine—the legal principle under which law enforcement can obtain information from commercial entities without a warrant. From a technical perspective, much consideration has been paid to two countervailing and concurrent trends: the rise of the "golden age for surveillance," in which law enforcement access to information is greatly enhanced through the availability of enormous amounts of commercially collected information, and the "going dark" problem, in which law enforcement can no longer access communications information previously available, due to encryption.[1] While much of the discussion of the role of commercial practices has focused on how businesses facilitate government access to information, attention has recently turned to the ways in which companies—particularly large digital communication companies—may limit law enforcement access to information.[2]

While these debates have engaged with a significant number of important policy issues that affect a broad range of stakeholders, an important issue has so far been left out of the discussion. Policy-makers and scholars often differentiate between intelligence gathering agencies and law enforcement agencies, but rarely consider how variation across different types of law enforcement agencies may affect their interactions with digital communication companies and their ability to obtain commercially collected information. However, there are a multitude of law enforcement agencies in the United States. They serve different communities, can avail themselves of different resources, and are subject to different restrictions. While the variation in law enforcement agencies can be understood in a number of ways, a particularly

important distinction is between agencies that serve large communities and agencies that serve small and midsize communities. These agencies differ in several key respects that may result in differences in their ability to obtain information from digital communication companies. If these differences are not considered, we run the risk of encouraging policies that will only work as expected in the context of law enforcement agencies that serve large communities.

This paper focuses on how efforts to limit law enforcement access to consumer data can have a greater impact on law enforcement agencies in small and midsize localities than on law enforcement agencies in large localities. Although law enforcement access to commercially collected information is mediated by a wide range of actors using a variety of mechanisms, I focus on efforts by digital communication companies to restrict access to information they have collected about their customers, as small and midsize police departments may have particular difficulties responding to these efforts. In conducting this analysis, I assume that the goal of surveillance regulation is not to minimize the information collected by law enforcement, but rather to ensure that privacy rights are protected while allowing law enforcement agencies to collect information as effectively and efficiently as they can, pursuant to appropriate legal procedures.

I begin by exploring variations between small and midsize law enforcement agencies and large law enforcement agencies and discussing how they may result in variations in how they conduct investigations. I then analyze how efforts by digital communication companies to limit the information they provide to law enforcement can differentially affect small and midsize law enforcement agencies. Finally, I conclude by discussing the negative policy outcomes that are likely to ensue and briefly suggesting pathways for ameliorating these harmful effects without losing the societal benefits created when digital communication companies resist law enforcement access to consumer information.

Overview of Variation in Law Enforcement Agencies

There are over seventeen thousand state and local law enforcement agencies in the United States.[3] In contrast to law enforcement in many other countries, policing in the United States is intensely localized. "There is no single universal formula for how a police department should look and operate; rather policing should be responsive to and shaped by local circumstances."[4] Unsurprisingly, state and local law enforcement agencies across the country are as different as the communities they serve. While this localization allows law enforcement agencies the flexibility to meet the needs of their communities, it also creates variation in police capabilities and capacities across different localities—including differences in their ability to adapt to changes in technology. Even if changes in commercial data collection or encryption practices are implemented uniformly across the country, the ability of a particular law enforcement agency to respond and adapt to these changes will mediate their impact.

In this section, I describe variation in law enforcement agencies, paying particular attention to characteristics that might affect use of commercially collected information. While there are many ways to describe variation among law enforcement agencies, I focus on one that is particularly salient in the context of law enforcement use of information collected by digital communication companies: the size of the community served by the law enforcement agency. Consequently, I discuss how police departments in large cities and small towns vary in three key respects: investigations and activities undertaken, organizational structure and officer specialization, and engagement with interagency resources and task forces. This analysis highlights key differences between law enforcement agencies that serve different sizes of localities that may result in differences in their ability to respond to changes in consumer technology.

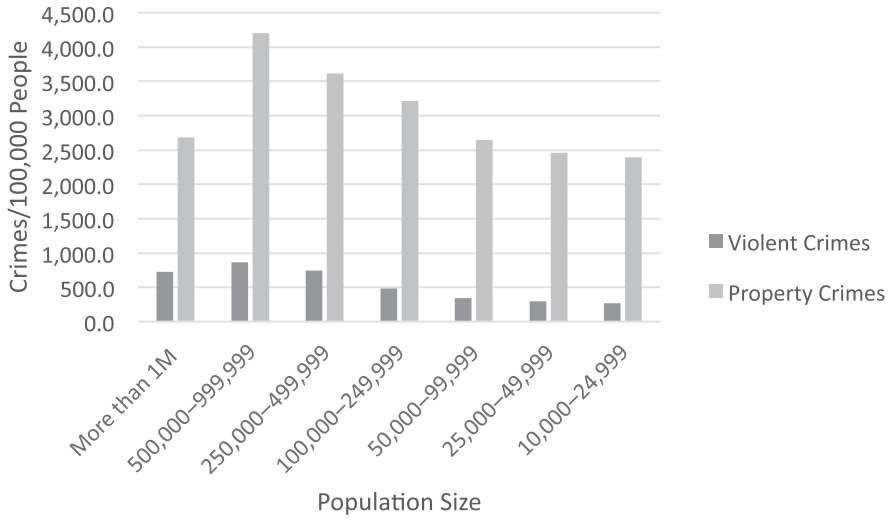
When taken as a whole, this analysis suggests that law enforcement agencies in large cities have more opportunities to investigate crimes using commercially collected information, and the expertise they develop as a result of these repeated investigations is more likely to be concentrated in fewer, more specialized officers. While law enforcement agencies in small and midsize cities can—and do—enhance their capabilities by cooperating with other agencies, these interagency activities do not completely replicate the experience of large law enforcement agencies.

Differences in Investigations and Other Activities

Law enforcement departments that serve small and midsize communities investigate fewer serious crimes than their big-city counterparts. As shown in figure 1 below, data from the Uniform Crime Reports (UCR) demonstrate that localities with greater populations generally have higher rates of both violent and property crimes.[5] As urban law enforcement departments are called upon to investigate more crimes—both proportionally to their population and in absolute number—these departments have more opportunities to request obtaining commercially collected information about individuals. However, the relationship between population size and crime rates should not be overstated. Crime rates do not strictly increase with locality size: for example, the crime rate for cities with populations between 500,000 and 999,999 people is higher than the crime rate for cities with populations of more than a million people. Additionally, many factors besides population size affect levels of criminal activity. Localities with similar population sizes may have widely different crime rates.

Research into variation across law enforcement agencies supports this evidence from the UCR and suggests that differences between activities conducted by small/midsize police departments and large police departments extend beyond the number of crimes they investigate. A study of calls-for-service received by a selection of urban and small-town police departments revealed that, "while the majority of law enforcement-related calls handled by both the urban and the small town agencies dealt with minor offences, the urban agencies generally dealt with slightly higher proportions of serious crimes."[6] Relatedly,

Figure 1: 2016 Crime Rates, by Population Size



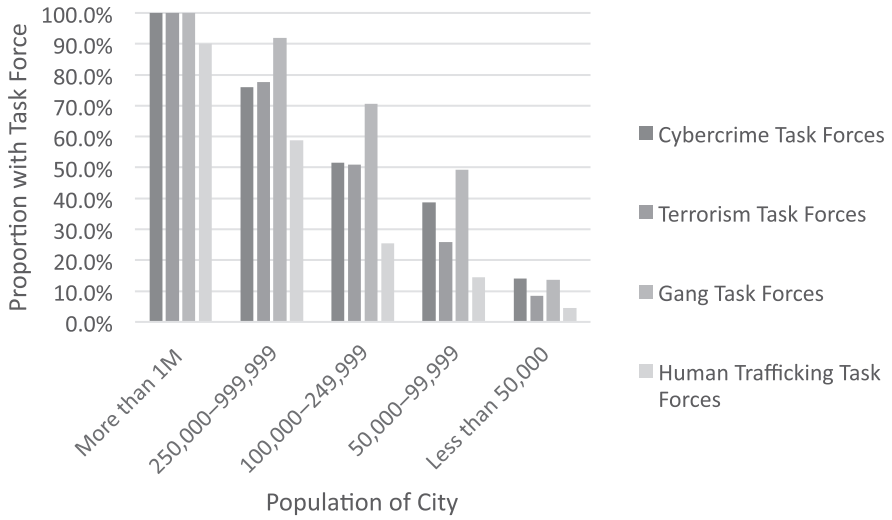
Source: Federal Bureau of Investigation, *2016 Crime in the United States,* https://ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016 (2017).

the size of an agency may also affect the salience of different public safety challenges. An analysis of grant applications from rural and suburban police departments revealed that larger agencies may be more concerned with "serious crime issues," such as violent crimes, and less concerned with public order-type crimes, such as vandalism.[7]

Police departments in small and midsize communities may also be less likely to engage in counterterrorism and homeland security activities, possibly because they have fewer resources available to devote to these efforts. In a study of small law enforcement agencies in Illinois, Schafer, Burruss, and Giblin found that agencies in small communities "reported struggling to secure training, equipment, and other resources to enhance homeland security efforts, though open comments suggested variation in whether this was actually a cause for concern for agency representatives."[8]

As data are not available on the number of requests for commercially collected information made by particular localities, it is difficult to tell whether differences between the activities undertaken by large urban police departments and police departments in smaller cities result in variation in the number of requests for consumer information. However, differences in the investigations and activities conducted by these agencies suggest that law enforcement agencies in large communities may have greater demand for commercially collected information. Police departments in large localities investigate a greater number of crimes, investigate more serious crimes, and are more likely to be involved in homeland security-oriented actions. Commercially collected information could play a vital role in all of these activities. In contrast, police departments that serve smaller communities investigate proportionally fewer crimes and devote more attention to informally addressing incidents

Figure 2: Use of Specialized Task Forces, by Population Size



Source: US Department of Justice, "Law Enforcement Management and Administrative Statistics (LEMAS), 2013," www.icpsr.umich.edu/icpsrweb/NACJD/studies/36164.

of public disorder and dysfunction.[9] Consequently, even though commercially collected information can play a vital role in investigating serious criminal activity, small and midsize police departments may request this information less often.

Differences in Organizational Structure and Career Paths

Police departments that serve larger communities must employ more officers than their small and midsize counterparts. While this increased manpower is necessary to handle the needs of a larger population, it also allows officers from large police departments to serve in a more specialized capacity—and consequently to develop more specialized expertise. Data from the most recent edition of the Law Enforcement Management and Administrative Statistics (LEMAS) dataset demonstrate that law enforcement agencies that serve larger communities have a greater number of specialized task forces.[10] Among the cities surveyed for this study, police departments in cities with populations of more than one million people have, on average, more than thirty specialized task forces devoted to investigating certain types of crimes, while police departments in cities with populations between 50,000 and 250,000 have fewer than five on average. Furthermore, as shown in figure 2 above, cities with greater populations are more likely to have tasks forces conducting investigations into crimes that are highly likely to involve data developed from consumer devices.[11]

Task forces allow police departments to cultivate and concentrate expertise in several ways. Officers on these task forces repeatedly investigate similar crimes, allowing them to learn more about how those crimes are committed, what practices are common among those who commit those crimes, and what investigatory tools are most likely to yield information

about these criminal practices. Additionally, by engaging with other officers who routinely conduct similar investigations, law enforcement officers can learn from the experiences of their peers. While interactions with peers can be a vital source of information for all law enforcement officers, sharing best practices within task forces may be particularly useful as members of the same task force likely engage in similar activities and face similar challenges.[12] Interactions with peers may also influence officers' willingness to adopt new technologies, as officers can observe whether the new technology was useful to their peers.[13]

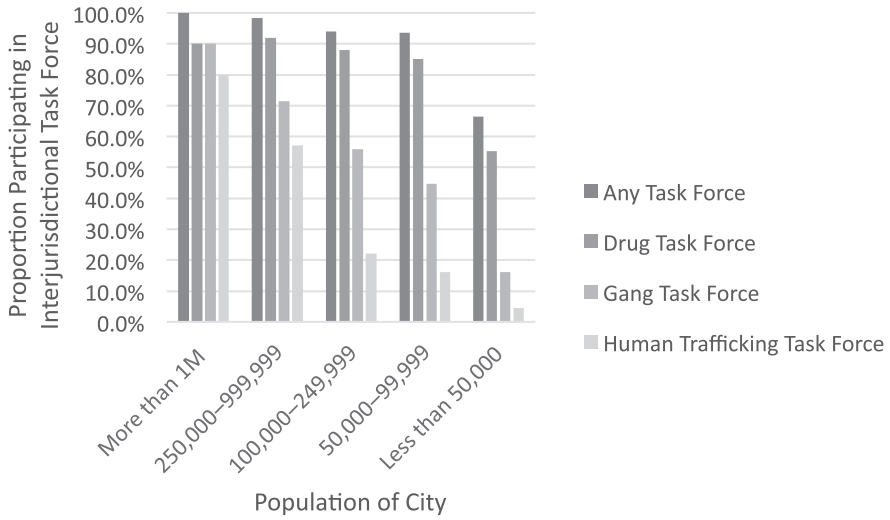
Studies of law enforcement career paths similarly demonstrate that officers from small and midsize communities appear more likely to engage in a broad variety of law enforcement activities and less likely to become specialists who focus on particular types of investigations. "Contrary to the concept of the urban professional-style police where specialization is perceived as a mark of professionalism, small-town police officers must be generalists who carry out full-spectrum police responsibilities."[14] Differences in specialization expectations between law enforcement officers from large cities and those from small/midsize towns may be in part due to the broader range of activities required of officers from smaller jurisdictions. Observational studies of law enforcement officers in small towns support the theory that "these officers . . . handle a wide range of problems, including those outside the realm of law enforcement."[15]

In sum, not only do police departments in large cities investigate more crimes than police departments in small/midsize communities, but they distribute the work of investigating those crimes in a different manner. Larger law enforcement agencies are able to support more specialized task forces. Officers who serve on these task forces can more easily become specialists in conducting certain types of investigations—and consequently can more easily become specialists in the investigative techniques that are most useful during these investigations. Officers at small and midsize law enforcement agencies are instead incentivized to become generalists. Consequently, it may be harder for officers in smaller departments to develop specialized expertise and share that expertise with their fellow officers.

Interagency Sharing and Cooperation

Despite differences in service patterns and organizational structures, law enforcement agencies from a variety of jurisdictions share the common purpose of preventing and investigating crime. To fulfill this purpose, agencies can—and frequently do—share information and resources through a variety of formal and informal mechanisms.[16] Cooperation mechanisms may allow law enforcement agencies that serve smaller communities to economically develop shared expertise in investigating technical or complex crimes. They may also allow agencies that serve smaller communities to take advantage of the resources maintained in larger communities. Additionally, law enforcement agencies within a state may be required to engage with a state agency to conduct certain forms of surveillance, as state laws strictly limit use of

Figure 3: Participation in Interjurisdictional Task Force, by Population Size



Source: US Department of Justice, "Law Enforcement Management and Administrative Statistics (LEMAS), 2013," www.icpsr.umich.edu/icpsrweb/NACJD/studies/36164.

this surveillance.[17] While differences between law enforcement agencies in large and small/midsize cities may be mitigated by interagency cooperation, there are significant reasons to believe that interagency cooperation will not allow smaller departments to completely replicate the facilities of larger departments.

Data from LEMAS suggest that law enforcement agencies serving smaller communities are less likely to participate in task forces focusing on particular types of serious crimes or crimes that involve specialized types of investigation. As can be seen in figure 3 above, a majority of all cities surveyed by LEMAS participated in some form of interjurisdictional task force. However, participation was still more common among large cities than small and midsize cities. Furthermore, large cities were more likely to engage with a broader variety of interjurisdictional task forces, thus increasing exposure to the resources available through interjurisdictional task forces.

Furthermore, law enforcement agencies that rely on shared resources to conduct surveillance are more likely to face delays due to the limited capacity of those resources. These delays may also occur in circumstances where state laws may only allow certain forms of electronic surveillance to be used by designated state law enforcement agencies, thereby requiring local law enforcement to collaborate with state officials to use these forms of surveillance. Centralization can concentrate electronic surveillance equipment and expertise at the state level, facilitating effective, efficient, and appropriate use of surveillance. However, centralization may also introduce surveillance bottlenecks: places where limited technical capacity may impede government efforts to use electronic surveillance. For example, under

the Texas Code of Criminal Procedure, wiretaps must be implemented by the Department of Public Safety.[18] Consequently, the Department of Public Safety's capacity to conduct wiretaps determines how many wiretaps can be utilized by all law enforcement agencies in the state of Texas.

Efforts by Digital Communication Companies to Constrain Law Enforcement Access to Consumer Information May Disproportionately Affect Investigations by Small and Midsize Agencies

Digital communication companies that obtain consumer data can use several mechanisms to make it more difficult for law enforcement officers to obtain information about their customers. In a recent article, Alan Rozenshtein analyzed how such companies might resist government surveillance, noting that "large powerful companies that stand between the government and our data and, in the process, help constrain government surveillance" serve an important role as "surveillance intermediaries."[19] While large-scale commercial collection of data about individuals may provide law enforcement with information it could not previously access, digital communication companies can act within the discretion available to them to make it more difficult for law enforcement to obtain this information, in part by strictly insisting on legal process prior to providing information and narrowly interpreting what information they are required to provide in response to a request.[20] Furthermore, just as privacy is protected through both legal processes and practical restrictions on law enforcement's ability to obtain data, digital communication companies can also select their practical processes to make it more difficult for law enforcement to request and obtain information about their customers.[21]

However, strengthening these barriers may not affect all types of law enforcement departments equally. As police officers in small and midsize jurisdictions investigate different crimes, engage in different activities, and follow different career paths, they may be less able to adapt to the changing behavior of digital communication companies than their colleagues in large cities. Consequently, actions by digital communication companies that are neutral on their face may in practice have an outsize impact on certain law enforcement agencies. In the remainder of this section, I describe how increased enforcement of both legal and practical procedural barriers may disproportionately affect law enforcement agencies in small and midsize communities and how law enforcement agencies in small and midsize communities may be less able to seek alternative sources of information if they cannot obtain information collected by digital communication companies.

Law enforcement in small and midsize cities may have more difficulty adapting to changes in enforcement of procedural barriers

Law enforcement access to information collected by digital communication companies is mediated by both legal and practical processes. Law enforcement efforts to obtain consumer

information from digital communication companies are regulated by federal and state law. Under federal law, police officers must obtain a warrant before compelling disclosure of the contents of a consumer's stored communications.[22] They must get a court order based on specific and articulable facts before compelling disclosure of most consumer records.[23] And they need a subpoena before compelling disclosure of basic user information such as the consumer's name and address.[24] In addition, state law may require state and local law enforcement within that state to comply with stricter protections for consumer information. For example, California recently passed the California Electronic Communications Privacy Act (CalECPA), amending its criminal procedure statute to require law enforcement to obtain a warrant prior to compelling disclosure of electronic communication information, defined broadly to include a wide range of information related to the communication, including "the location of the sender or recipients at any point during the communication."[25] While companies may cooperate with law enforcement requests on a voluntary basis, the prevailing trend is for digital communication companies to require formal legal process prior to providing information to law enforcement.[26]

Within this legal framework, digital communication companies can make the process by which law enforcement obtains information more difficult in several ways. Alan Rozenshtein refers to this practice as proceduralism: digital communication companies restrict law enforcement access by requiring formal legal process before turning over any information, and even then only releasing the minimal amount of information necessary to comply with the request.[27] Efforts to restrict the information released to law enforcement by narrowly interpreting legal orders may benefit society by ensuring that law enforcement information requests are narrowly framed and factually supported. But they can also impose significant delays on investigations if law enforcement officers must submit multiple requests before they obtain the information they seek from digital communication companies.

Complying with applicable legal requirements is a necessary but not sufficient component for law enforcement to obtain information from commercial companies. Law enforcement officers also face several practical barriers to obtaining and utilizing information from digital communication companies. Before they can seek information, law enforcement officers must realize that information relevant to their investigation has been collected by a digital communication company and then identify the company (or companies) likely to hold the information. Officers must then determine how to technically specify the scope of the information they seek, determine what form of legal process is appropriate, and develop evidence sufficient to support their request. They must then present the request for information to the company. The company may comply with the request—or it may object if it feels the request is defective in some way. Once the law enforcement agency obtains information, it must analyze it in order to determine how it should be used in the investigation. Although some of these steps may seem trivial, each has the potential to pose significant difficulties under the right set of circumstances.[28]

Just as digital communication companies can decrease law enforcement access to consumer data by narrowly interpreting their legal obligations, they can also decrease access by making it more difficult for law enforcement officers to request information as a practical matter. Digital communication companies can make it more or less difficult for police officers to contact them by selecting the forums through which law enforcement officers can make a request. For example, law enforcement officers request information from Snapchat by emailing a written request accompanied by appropriate legal process, while both Facebook and Twitter have specialized online request forms that law enforcement officers can use to submit requests.[29] Digital communication companies may also produce sample documents or templates, providing law enforcement with examples of what the particular company considers to be sufficient specificity.[30] The use of online request forms and sample documents lowers the practical barriers for law enforcement officers seeking commercially collected information and may also allow digital communication companies to shape the requests they receive from law enforcement to ensure that these requests are adequate and sufficiently narrow.[31] This promotes efficiency for both the digital communication company and the police by increasing the likelihood that appropriate requests are made without repeated submissions. A company that wishes to make it as difficult as possible for law enforcement to obtain data may elect not to provide any such guidance. Furthermore, digital communication companies also have some discretion in how quickly they respond to law enforcement requests. Companies that do not wish to release information may elect not to expedite requests.

Although not itself a digital communication company, 23andMe provides an illustration of how companies can create practical barriers to discourage law enforcement requests for customer information. 23andMe, a company that provides genetic testing services directly to individuals seeking to learn more about themselves or their ancestry, has explicitly stated that they "unequivocally choose to use all practical legal and administrative resources to resist requests from law enforcement."[32] Consequently, 23andMe will only accept written law enforcement requests "submitted by certified mail, express courier, or in person."[33] Furthermore, while 23andMe's law enforcement guidelines state it will reject overly broad requests, it provides very little information about the specific details required to fulfill a request.[34] Perhaps unsurprisingly, 23andMe has received very few law enforcement requests. As of the publication of its December 2017 transparency report, it has provided no consumer information in response.[35]

While digital communication companies can reduce police access to the data they collect by making both their legal and practical processes more difficult to navigate, law enforcement officers are able to learn from their prior experience with digital communication companies to minimize the delay and hassle caused by proceduralism. When a law enforcement officer requests information from a company, she can use her prior experiences with the company to maximize the likelihood that her request will return the information she seeks. When the law enforcement officer has the option of seeking information from multiple companies,

she can use her experience to prioritize requests to those companies that are likely to produce responsive information most quickly. The officer can share this information with her colleagues, and similarly benefit from their experiences.

However, this learning process will occur more efficiently and effectively in law enforcement agencies in large cities. Such agencies conduct more serious criminal investigations in a year, both because they serve more people and because, on average, their communities have higher crime rates. Additionally, because officers in urban law enforcement agencies are more likely to specialize in solving particular types of crime, they are more likely to interact repeatedly with the particular digital communication companies used by the criminals they are investigating. Consequently, some law enforcement officers who serve in large agencies are able to develop specialized expertise in requesting information from digital communication companies, despite efforts by the companies to limit the information obtained.

Because law enforcement officers in small and midsize departments develop more generalized expertise, they have fewer opportunities to repeatedly engage with particular digital communication companies. Furthermore, they are likely to work with a smaller group of colleagues, who have similarly generalized expertise. While there are some digital communication companies whose services are so ubiquitously used that even an officer who infrequently requests information from commercial entities is likely to contact them multiple times, these are also the companies with the greatest incentives to push back against law enforcement information requests.[36]

Furthermore, large cities have greater abilities and incentives to push back when they believe that a digital communication company has not provided sufficient information subject to a lawful court order. Just as large digital communication companies are better positioned than small digital communication companies to litigate orders to release consumer information, large law enforcement departments are better positioned to litigate circumstances where a company refuses to comply with a court order than small departments.[37] Large law enforcement departments likely have more resources and are thus better able to support extensive litigation activities. Large law enforcement departments more frequently request information from digital communication companies, and are therefore able to select a case that best presents their argument. Finally, large departments are more incentivized to pursue litigation, as they request information more often and therefore have more to gain from increased access to information collected by digital communication companies. The greater ability of large law enforcement agencies to litigate court orders may collaterally help smaller law enforcement agencies, to the extent that they are able to free ride on changes in law brought about by this litigation.

To see how changes in proceduralism—especially by large digital communication companies—may differentially affect the ability of law enforcement officers in small and

midsize communities, consider two identical, hypothetical investigations: one conducted by an officer in a large city and one conducted by an officer in a small town. Each officer is investigating a violent robbery and has identified a suspect. The police believe that the victim was selling drugs to the robber when the robber attacked him, stole the drugs and a watch the victim was wearing, and viciously beat the victim. Due to the nature of the crime, the victim refuses to cooperate with police. Therefore, in order to learn more about interactions between the victim and the suspect, the police decide to seek information from digital communication companies. In order to do this, the officers must first identify companies that are likely to have collected information from the suspect relevant to the investigation, determine how to technically specify the information they seek, and identify the correct legal process for obtaining the information.

The police officer investigating this crime in a large city is likely to be highly specialized—devoting all of her time to investigating robberies or other similar, serious crimes. She is therefore well versed in identifying what information she can obtain from commercial entities to help her make her case and has repeatedly interacted with these companies in the past. Furthermore, this officer likely has a large group of colleagues who investigate similar crimes, and consequently may be able to share insights about how to obtain information from a particular company. When a digital communication company attempts to reduce law enforcement's access to information it has collected from its customers by increasing enforcement of procedural and practical barriers, the police officer in the large city is likely to notice the shift immediately. However, she can also quickly learn what is now necessary to overcome those new barriers. The officer frequently requests information from digital communication companies and therefore chooses the company she believes will provide the information she seeks with the least amount of hassle. Because she frequently requests information from this particular digital communication company, she may have a preexisting contact at the company who can help her understand and navigate the new rules. She can also rely upon the experiences of her numerous colleagues, who also frequently request commercially collected information, to learn what is now needed to obtain information from the digital communication company without undergoing her own process of trial and error. Consequently, although the big-city officer is affected when the digital technology company increases its procedural barriers, she is quickly able to minimize this impact and continue obtaining information. She is able to efficiently comply with the procedural barriers because her frequent interactions with the digital communication company leave her with little uncertainty about the procedures that apply and the best way to satisfy them.

In contrast, an identical robbery committed in a small locality is likely to be investigated by a less specialized officer. While this officer is highly likely to serve in a primarily investigatory capacity, he is likely to investigate a wider variety of crimes and consequently use a wider variety of investigative techniques. Furthermore, he is likely to have fewer colleagues who investigate similarly serious crimes and is much less likely to participate in a task force that

specializes in investigating related crimes. The officer investigating the robbery in the smaller jurisdiction therefore has fewer opportunities available to learn how to efficiently respond to strict enforcement of procedural barriers by digital communication companies. As he requests commercially collected information less often, it will be more difficult for him to identify the company that will provide the information with the least amount of hassle. He may be less aware of the idiosyncratic methods of specifying information required by a particular company or of the particular processes that it is least likely to object to. He is also less likely to have an established point of contact at the company, whom he knows will respond quickly to his questions. As procedural and practical barriers increase, he must engage in a longer process of trial and error to successfully request information. This can both increase the cost of obtaining information and create delays in the investigation. While the officer can rely on the experiences of his colleagues when seeking this information, he is likely to have fewer colleagues who frequently request this information from a particular digital communication company. Formal and information-sharing mechanisms can enable him to learn from the experiences of others in other jurisdictions. But these mechanisms may take time and be less effective. The officer will be able to apply his experience in requesting the information to future investigations. However, he may have fewer opportunities to do so than a comparable officer in a large city, since he investigates a broader variety of crimes.

In sum, although the police officer in the smaller jurisdiction faces the same procedural barriers as the officer in the larger jurisdiction, the process of overcoming those barriers is less efficient in the smaller jurisdiction. The police officer in the smaller jurisdiction has more uncertainty about the response of the digital communication company to his request and fewer opportunities to reduce that uncertainty through firsthand experience or learning from his colleagues. Although digital communication companies may change their reliance on legal and practical barriers uniformly for all law enforcement agencies, police departments that serve smaller communities are disproportionately affected by these changes.

Law enforcement in small and midsize cities may be less able to pursue alternative means of obtaining information

As digital communication companies use legal and practical means to push back against government requests for customer information, law enforcement agencies may explore other sources for the information they seek. Law enforcement could seek information from other companies, who may obtain information comparable to that obtained by large digital communication companies but have fewer incentives and resources to deny law enforcement access. Alternative sources of information could include both smaller digital communication companies and companies that do not provide digital communication services directly to consumers. Alternative sources of commercially collected data are especially likely when police officers target information collected

through a mobile device, as mobile devices often transmit information to multiple entities simultaneously—with or without the conscious knowledge of the mobile device user.[38]

Although seeking information from companies other than large digital communication companies would seem to require few resources, there are still significant barriers to obtaining this information. Law enforcement officers must be able to identify which companies are likely to have the information they seek. This can be particularly difficult when officers seek to request user data from small mobile app developers. It may not be clear—either to the user or law enforcement—what information has been collected by a particular app. Mobile app companies may not anticipate receiving law enforcement information requests and therefore may not have internal processes set up to manage and respond to the request. Consequently, it may be difficult for law enforcement to determine where and how to submit the request or determine how long a response to the request is likely to take.

While these factors may affect both large and smaller law enforcement departments, they are likely to have a greater impact on smaller law enforcement departments. Because large departments have more experience using commercially collected information, it will be easier for them to identify smaller companies that might have the information they seek. Based on their prior investigations, a unit within a large law enforcement agency that investigates a particular type of crime may be able to readily identify apps that are commonly used to commit those crimes. For example, a narcotics unit may be acutely aware of changes in the apps that drug dealers use to communicate with their suppliers. Larger law enforcement departments may also have experience with the smaller companies in question, which may make it easier for them to request information and provide them with some insight into whether the smaller company is likely to have the information in question.

In addition to finding other companies that may have collected the information they seek, law enforcement agencies could attempt to use other forms of surveillance or information-gathering to replace the information they could have obtained from the communication company. Rather than relying on commercially collected information generated by a device, law enforcement agencies may attempt to directly access the device itself—which may be encrypted or otherwise inaccessible.[39] Law enforcement could also seek to conduct its own electronic and physical surveillance, if it is unable to obtain location information from a digital communication company. However, alternative methods of obtaining information are generally more controversial, more expensive, or more dangerous.[40] Additionally, if law enforcement agencies must make a factual showing to a judge before using these other forms of surveillance or information-gathering, it may be more difficult for them to do so if they cannot first obtain commercially collected information to support their request.

While law enforcement may be able to obtain the information it seeks without the assistance of digital communication companies by using other forms of surveillance, large law enforcement departments are better situated than small and midsize departments to use these alternatives, for several reasons. Large police departments may be better able to access encrypted devices using encryption workarounds, which require significant resources and expertise. "The toolkit of encryption workarounds varies considerably, depending on which government agency is investigating and how important any particular case happens to be."[41] Furthermore, encryption workarounds will not always allow the police to access the device: they may be successful under some circumstances but not others.[42] Law enforcement officers in large departments may also have more ready access to electronic surveillance tools, such as cell-site simulators, that they can use to directly obtain information about a target.

To see how officers in smaller jurisdictions may be less able to pursue alternative means of obtaining information, let's return to the previously discussed hypothetical case concerning the police officer from the large city and the police officer from the small locality, each investigating identical violent robberies. When the police officer in the large jurisdiction is unable to quickly obtain information about her suspect from a large digital communication company, she turns to her coworkers to ask whether they have suggestions about other companies that may have collected information about her suspect. A colleague suggests that she try a new app that allows users to post pictures of luxury goods. While the pictures are always made publicly available, people can use private chat functions to communicate about the goods. The police officer's colleague has realized that people in their city often use this app to fence stolen goods and that the suspect may have posted pictures of the watch if he is interested in selling it. The police officer looks through the pictures publicly available on the app and is able to identify the victim's watch. She then goes to the app developer with a court order and requests information about the account that posted pictures of the watch, including the location from which the posts were made. The app developer receives very few law enforcement requests, and consequently does not have existing policies that make it difficult for law enforcement to obtain information. Instead, he simply wants to provide the information required with as little fuss as possible so that he can continue to develop and grow his business. She is then able to determine that the user of the account frequently makes posts from the suspect's home, which provides her with information she is able to use to support either another request for information from the digital communication company or a request for a warrant to seize and search the suspect's mobile device. Furthermore, she anticipates that she may have trouble accessing the suspect's device due to encryption, and consequently plans a diversion in advance so that she can seize the device from the suspect while it is unlocked and he is using it.[43] She is able to successfully obtain and access the device and proceed forward with her case. While her inability to access information about the suspect directly from a digital communication company has caused some delay and increased hassle, she is ultimately able to obtain access to the suspect's phone—a powerful source of evidence in criminal cases.

In contrast, the police officer in the smaller jurisdiction may have more difficulty identifying a useful alternative source of commercially collected information. Because he does not exclusively investigate robberies, he may be less familiar with which obscure mobile app people use to sell stolen goods. He can consult with colleagues in his department—who are also less likely to be familiar with the apps because of their more generalized investigative expertise—and with law enforcement officers from other jurisdictions. He eventually contacts a colleague in a different department, who reports that he has noticed that a particular mobile app is frequently used to seek buyers for stolen goods. The police officer is therefore able to contact the mobile app and obtain information in much the same way as his big-city counterpart. However, his investigation has experienced some delay because it has taken him longer to identify the alternative source of commercially collected information. After obtaining information about the suspect from the mobile app developer, the police officer from the smaller jurisdiction is similarly able to obtain a warrant to seize and search the suspect's mobile phone. While he anticipates that the phone may be encrypted, he is less familiar with the workarounds he can use to obtain information from the phone. Consequently, the risk that he will not be able to access the device due to encryption is higher than that faced by the police officer investigating a similar crime in a larger jurisdiction.

Overall, both police officers are able to explore alternative methods of obtaining information that they cannot obtain from digital communication companies in a timely fashion. Both police officers face delay and uncertainty in whether these alternative methods will be successful. However, the police officer in the smaller jurisdiction is likely to face more delays, as he must engage in more information-seeking to identify other companies that may have collected the information he seeks. The police officer in the smaller jurisdiction may also face more uncertainty about the success of alternative techniques for obtaining information. This is particularly true if the police officers must rely on encryption workarounds, which are inherently probabilistic and may require "technical expertise and deep pockets."[44]

Policy Implications of Differences in Access to Information Collected by Digital Communication Companies

Even if efforts by digital communication companies to limit law enforcement access to information affect small and midsize law enforcement agencies more than large law enforcement agencies, it is reasonable to ask whether these differences will result in negative policy outcomes. If large law enforcement departments investigate more crimes and—presumably—request information more frequently from digital communication companies, it may be optimal for these companies to establish policies based on their interactions with law enforcement agencies in large communities. However, there are several negative policy outcomes that may ensue if law enforcement from small and midsize communities cannot effectively access information collected by digital communication companies.

First, loss of access to information collected by digital communication companies may hamper criminal investigations conducted in smaller localities. A significant number of serious crimes occur every year in small and midsize localities, even if the rate at which they occur is lower than that faced by large cities. In 2016, more than 2,500 incidents of murder/nonnegligent manslaughter, 47,000 incidents of robbery, and 150,000 incidents of aggravated assault occurred in localities with fewer than fifty thousand inhabitants.[45] Increased restrictions on law enforcement access to information collected by digital communication companies would undoubtedly create difficulties in some of these investigations. While digital communication companies' efforts to restrict law enforcement access to information would have an impact on comparable investigations in large law enforcement departments, this impact would be more deeply felt by small and midsize agencies. Additionally, small and midsize agencies would be less able to compensate for the loss of this information by seeking comparable information from different companies.

Second, while small and midsize localities may be denied the benefits of law enforcement access to information collected by digital communication companies, larger jurisdictions will experience more of the harms associated with access to this information. An increased difference between the information-gathering abilities of agencies in large cities and agencies in small and midsize cities exacerbates existing inequities in who is subject to surveillance. Large law enforcement agencies already have more extensive surveillance capabilities and expertise than agencies in small and midsize communities. Even if digital communication companies reduce the amount of information that can be obtained by law enforcement agencies in both small and large communities, if the reduction is greater in small communities it will increase the inequality already present between small and large communities.

Third, increasing the difference between the information that can be obtained by large law enforcement departments and the information that can be obtained by small and midsize departments can warp our understanding of both the current state of surveillance and the options for reform. In general, information about surveillance conducted by law enforcement departments in large cities is more likely to become public knowledge, due to increased interest by advocacy groups and increased likelihood of litigation. Consequently, as differences increase between the surveillance capabilities of departments in large communities and departments in small communities, our understanding of how surveillance is actually conducted across the country becomes increasingly inaccurate. Furthermore, when we consider potential policy innovations to better protect individual privacy or more efficiently regulate law enforcement surveillance, we are likely to obtain a less optimal policy outcome as our knowledge about surveillance practices becomes less accurate.

Given that it appears that attempts by digital communication companies to restrict law enforcement access to consumer information may disproportionately affect agencies in

small and midsize communities, resulting in negative policy outcomes, the next step may be to determine what could be done to mitigate these outcomes. While these outcomes could be avoided by digital communication companies resuming their prior practices of not aggressively challenging law enforcement access to information, this path would also result in the loss of the significant societal benefits that accompany the additional regulation of law enforcement surveillance. However, there are several options that would allow us to maintain the benefits of increased surveillance regulation while avoiding the negative consequences of increased inequality in law enforcement access to information. For example, improved and formalized mechanisms for information-sharing among law enforcement departments may help small and midsize departments adapt to changes in digital communication companies' expectations more quickly.

Digital communication companies themselves have several options for mitigating the distributional effects resulting from their efforts to protect their customers' information. One possibility would be for digital communication companies to standardize practices across their industry, thus decreasing the learning curve for law enforcement. However, this cooperation may be both controversial and logistically difficult. Another option would be for digital communication companies to release more detailed information about the requests they receive from law enforcement, including information about the law enforcement agencies that make these requests. Although this information would not reduce unequal access to information, it would provide a more accurate picture of variation in requests for information by different types of law enforcement agencies, therefore providing a more accurate picture of surveillance across the United States.

No matter what, if any, future action is taken to mitigate the differential effects of efforts by digital communication companies to limit law enforcement access to the data they collect about their customers, simply acknowledging that these differences exist will put us in a better position to understand the impact of our policy decisions. The first step toward crafting surveillance policy that serves all communities is understanding the differences between those communities. Without this knowledge, we may end up with policies that only serve those few jurisdictions that frequently request information from digital communication companies.

NOTES

1 Peter Swire and Kenesa Ahmad, "Encryption and Globalization," *Columbia Science & Technology Law Review* 13 (2012): 416, 466–70; James B. Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" Presentation to the Brookings Institution, October 16, 2014, accessed January 18, 2018, https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

2 Alan Rozenshtein, "Surveillance Intermediaries," *Stanford Law Review* 70 (forthcoming 2018): 5.

3 Brian A. Reaves, "Census of State and Local Law Enforcement Agencies, 2008," Bureau of Justice Statistics, 2011, accessed January 18, 2018, https://www.bjs.gov/content/pub/pdf/csllea08.pdf.

4 L. Edward Wells, David N. Falcone, and Cara Rabe-Hemp, "Community Characteristics and Policing Styles in Suburban Agencies," *Policing: An International Journal of Police Strategies and Management* 26, no. 4 (2003): 566.

5 Federal Bureau of Investigation, "2016 Crime in the United States," 2017, accessed January 18, 2018, https://ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016.

6 Richard R. Johnson and Trisha N. Rhodes, "Urban and Small Town Comparison of Citizen Demand for Police Services," *International Journal of Police Science & Management* 11, no. 1 (2009): 27, 36.

7 Joseph B. Kuhns III, Edward R. Maguire, and Stephen M. Cox, "Public-Safety Concerns Among Law Enforcement Agencies in Suburban and Rural America," *Police Quarterly* 10, no. 4 (2007): 429, 441.

8 Joseph A. Schafer, George W. Burruss, Jr., and Matthew J. Giblin, "Measuring Homeland Security Innovation in Small Municipal Agencies," *Police Quarterly* 12, no. 3 (2009): 263, 283.

9 Brian K. Payne, Bruce L. Berg, and Ivan Y. Sun, "Policing in Small Town America: Dogs, Drunks, Disorder and Dysfunction," *Journal of Criminal Justice* 33, no. 1 (2005): 31, 34–38. Payne et al. analyzed police reports published in a newspaper in a small town in Pennsylvania, identifying four prominent trends in the situations the police department was called upon to address: issues related to animals (including lost pets or strays), disorderly behavior stemming from alcohol intoxication, incidents stemming from dysfunctional interpersonal relationships, and other instances of public disorder (including vandalism).

10 US Department of Justice, "Law Enforcement Management and Administrative Statistics (LEMAS), 2013," accessed January 18, 2018, www.icpsr.umich.edu/icpsrweb/NACJD/studies/36164. For purposes of this analysis, I focused on city-level law enforcement agencies only, and consequently excluded any state, county, or tribal agencies.

11 Cities were described as having a specialized task force if they reported having a special unit with either full-time or part-time personnel devoted to each crime type.

12 Anja J. Doornbos, Robert-Jan Simons, and Eddie Denessen, "Relations Between Characteristics of Workplace Practices and Types of Informal Work-Related Learning: A Survey Study Among Dutch Police," *Human Resource Development Quarterly* 19, no. 2 (2008): 129.

13 See, e.g., Paul Jen-Hwa Hu, Hsinchun Chen, Han-fen Hu, Cathy Larson, and Cynthia Butierez, "Law Enforcement Officers' Acceptance of Advanced E-Government Technology: A Survey Study of COPLINK Mobile," *Electronic Commerce Research and Applications* 10, no. 1 (2011): 6, 14. ("Social influences can enhance the impacts of perceived usefulness, but alone, they do not appear to drive user intentions or actual technology usage.")

14 David N. Falcone, L. Edward Wells, and Ralph A. Weisheit, "The Small-Town Police Department," *Policing: An International Journal of Police Strategies and Management* 25, no. 2 (2002): 371, 376.

15 John Liederbach and James Frank, "Policing Mayberry: The Work Routines of Small-Town and Rural Officers," *American Journal of Criminal Justice* 28, no. 1 (September 2003): 53, 69.

16 Steven Chermak, Jeremy Carter, David Carter, Edmund F. McGarrell, and Jack Drew, "Law Enforcement's Information Sharing Infrastructure: A National Assessment," *Police Quarterly* 16, no. 2 (2013): 211; Alexander Weiss, "Informal Information Sharing Among Police Agencies," National Institute of Justice (December 1998), accessed January 18, 2018, https://www.ncjrs.gov/pdffiles/fs000233.pdf.

17 Jeff Strange, "*The Prosecutor* 39 (July-August 2009), accessed January 18, 2018, https://www.tdcaa.com/node/4813.

18 Texas Code of Criminal Procedure, Art. 18.20 § 5. ("only the Department of Public Safety is authorized . . . to own, possess, install, operate, or monitor an electronic, mechanical, or other device" used to intercept communications.)

19 Rozenshtein, "Surveillance Intermediaries," 5.

20 Rozenshtein, "Surveillance Intermediaries," 18–20.

21 Harry Surden, "Structural Rights in Privacy," *SMU Law Review* 60 (2007): 1605.

22 18 U.S.C. § 2703(a)-(b) (2017). However, it is possible for the government to obtain content information with a court order, if it provides prior notice to the customer whose information it seeks. 18 U.S.C. § 2703(b)(1)(B) (2017).

23 18 U.S.C. § 2703(c)-(d) (2017).

24 18 U.S.C. § 2703(c)(2) (2017).

25 California Penal Code § 1546-1546.1 (2017). However, law enforcement can still obtain basic subscriber information, such as a user's name, telephone number, or email address, with a subpoena. California Penal Code § 1546.1(i). For more information about CalECPA, including the exceptions to this requirement, see R. Taj Moore, "So What's in the California Electronic Communications Privacy Act?" *Lawfare* (blog), October 22, 2015, accessed January 18, 2018, https://lawfareblog.com/so-whats-california-electronic-communications-privacy-act.

26 Rozenshtein, "Surveillance Intermediaries," 10–11. Also see, e.g., Twitter, "Guidelines for Law Enforcement," accessed November 30, 2017, https://support.twitter.com/articles/41949#7. ("Non-public information about Twitter users will not be released to law enforcement except in response to appropriate legal process such as a subpoena, court order, or other valid legal process.")

27 Rozenshtein, "Surveillance Intermediaries," 18–19.

28 For a more complete discussion of the barriers law enforcement officers face when seeking commercially collected information, see Anne E. Boustead, "Police, Process, and Privacy: Three Essays on the Third Party Doctrine" (dissertation, Pardee RAND Graduate School, 2016), accessed January 18, 2018, https://www.rand.org/pubs/rgs_dissertations/RGSD384.html.

29 Snapchat, "Law Enforcement Guide," accessed January 8, 2018, https://www.snapchat.com/lawenforcement; Facebook, "Law Enforcement Online Requests," accessed November 30, 2017, https://www.facebook.com/records/x/login; Twitter, "Legal Request Submissions," accessed November 30, 2017, https://legalrequests.twitter.com/forms/landing_disclaimer.

30 For a detailed (but out of date) comparison of the processes by which digital communication companies field law enforcement requests, see Electronic Frontier Foundation, "Social Media—A Guide to the Law Enforcement Guides," 2011, accessed January 18, 2018, https://www.eff.org/files/eff_social_network_law_enforcement_guides-sprdsht.pdf.

31 As access to these pages is restricted to law enforcement personnel only, the exact content of these forms is unknown to me. Consequently, I am only talking about how creating an online form for law enforcement requests might allow a digital communications company to shape the requests it receives—not whether it does.

32 Kate Black and Zerina Curevac, "23andPrivacy: Your Data and Law Enforcement" (blog), accessed November 30, 2017, https://blog.23andme.com/23andme-and-you/23andprivacy-your-data-law-enforcement.

33 23andMe, "Guide for Law Enforcement," accessed November 30, 2017, https://www.23andme.com/law-enforcement-guide.

34 23andMe, "Guide for Law Enforcement."

35 23andMe, "Transparency Report," accessed November30, 2017, https://www.23andme.com/transparency-report.

36 Rozenshtein, "Surveillance Intermediaries," 13–14.

37 "Any surveillance intermediary can litigate a government order—but the biggest companies are best positioned to fight it out. Unlike small companies, they have the money for protracted litigation. And, as repeat

players, they have a key advantage over one-shot litigants: they have the luxury of choosing the best vehicle for legal argument." Rozenshtein, "Surveillance Intermediaries," 27.

38 Edward Balkovich, Don Prosnitz, Anne E. Boustead, and Steven C. Isley, "Electronic Surveillance of Mobile Devices: Understanding the Mobile Ecosystem and Applicable Surveillance Law," RAND Report No. RR800 (2015): 11, accessed January 18, 2018, https://www.rand.org/pubs/research_reports/RR800.html.

39 Indeed, commercially collected information is generally seen as a partial substitute for consumer devices that cannot be accessed due to encryption—not the other way around. See Matt Olsen, Bruce Schneier, and Jonathan Zittrain, "Don't Panic. Making Progress on the 'Going Dark' Debate," The Berkman Center for Internet & Society, February 1, 2016.

40 Rozenshtein, "Surveillance Intermediaries," 33; Kevin S. Bankston and Ashkan Soltani, "Tiny Constables and the Cost of Surveillance: Making Cents out of United States v. Jones," *Yale Law Journal* 123 (January 9, 2014): 335; Boustead, "Police, Process, and Privacy," 56–57.

41 Orin S. Kerr and Bruce Schneier, "Encryption Workarounds," *Georgetown Law Journal* (forthcoming, 2018): 34, accessed January 18, 2018, https://www.schneier.com/academic/paperfiles/Encryption_Workarounds.pdf.

42 Kerr and Schneier, "Encryption Workarounds," 4.

43 Kerr and Schneier, "Encryption Workarounds," 25–26.

44 Kerr and Schneier, "Encryption Workarounds," 33.

45 FBI, "2016 Crime in the United States."

The preferred citation for this publication is:
Anne E. Boustead, **Small Towns, Big Companies: How Surveillance Intermediaries Affect Small and Midsize Law Enforcement Agencies**, Hoover Working Group on National Security, Technology, and Law, Aegis Paper Series No. 1802 (February 8, 1018), available at https://lawfareblog.com/small-towns-big-companies-how-surveillance-intermediaries-affect-small-and-midsize-law-enforcement.

About the Author

ANNE BOUSTEAD

Anne Boustead is an assistant professor at the School of Government & Public Policy at the University of Arizona, where she researches surveillance, privacy, policing, and drug policy. She has a PhD from the Pardee RAND Graduate School, where her dissertation focused on law enforcement use of commercially collected data, and a JD from Fordham University School of Law.

Summary

This paper explores how efforts by companies to resist government requests for consumer information may disproportionately affect small and midsized law enforcement agencies, as small departments face obstacles to using commercially collected information that do not occur in the context of larger departments. Differences between law enforcement agencies that serve large communities and those that serve small communities suggest corresponding differences in their ability to adapt to changes in the process for obtaining data from digital communication companies. Failing to account for these differences may encourage policies that will only work as expected for large law enforcement agencies.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION