IN THIS ISSUE

Message from the Executive Director, 2
Fighting Corruption through International Cooperation, 4
Global Cooperative Efforts Required to Prevent Cybercrime, 8
Overcoming Hurdles to Secure Evidence from Social Media Companies in Cybercrime Investigations and Prosecutions, 13
Protecting the Public and Vulnerable Populations from Fraudulent Scams on Social Media, 18
Corporate and Government Responsibility to Protect Data and Assist Law Enforcement, 22
Recent Powers and Duties Decisions, 26
About the Authors, 31
In 2020, NAGTRI will host the tenth annual class of NAGTRI International Fellows. Some may wonder why state attorneys general need to partner with our international colleagues. But this partnership is an important effort for NAAG. To explain why, I will start with some NAAG history.

NAAG was created in 1907. The catalyst for its creation was the response of state attorneys general to the Standard Oil monopoly, which was unfairly crushing competition and causing huge market inefficiencies. Of course, the people who ultimately bore the brunt of this monopoly were consumers and businesses across the United States who paid much higher prices than they should have for oil and oil products.

So, in 1907 the state AGs from across the U.S. scheduled a meeting in St. Louis and founded NAAG. At the time, it was a serious and unusual thing for an AG to travel outside their state. Many of their constituents questioned why their AG should need to travel outside the state borders: how was that relevant to the problems being faced within their own state? Moreover, in those days, it took longer to get from Vermont or California to St. Louis then it now takes to travel from the United States to Singapore. But the United States, figuratively speaking, had shrunk, and what was going on in any one state was beginning to have a direct impact in others. State attorneys general could no longer operate in a vacuum. They needed to cooperate with each other across borders to face the new problems of their age.

Technological advances over the past several decades have now made the world a much smaller place. As the world shrinks, criminals have increasingly taken great advantage of the ability to easily commit crimes across borders. And even when crimes do not cross borders, the interconnections facilitated by the internet age have resulted in many similarities in the crimes committed wholly within individual nations. Like the attorneys general at the beginning of the 20th century, prosecutors and other government attorneys around the world in the 21st century have increasingly found that they do not exist within a vacuum in their own countries. As in 1907, when the AGs crossed new borders to come together and solve national problems that affected all of them, state attorneys general, through NAAG, are now stepping up to form international partnerships to help solve international problems that affect the citizens of their states. Working with our international partners makes both them and us better, helps keep us as Americans safe within our own borders, and is simply the right thing to do.

This issue of the NAGTRI Journal highlights the international work that NAAG is doing through the International Fellows program and through the NAGTRI Center for International Partnerships and Strategic Collaboration (CIPS-C). CIPS-C’s mission is to grow NAAG’s and NAGTRI’s international presence, build strategic partnerships in the global sphere, and provide training, technical, and research assistance to domestic and international government attorneys, prosecutors, and representatives to promote security and enhance capacity. The articles in this issue reflect the work of NAGTRI’s 2019 International Fellows and Gina Cabrejo, CIPS-C’s NAGTRI criminal justice instructor for Latin American programs. We hope you will find NAGTRI’s international efforts of interest.
NAGTRI Academy: Civility, Effective Leadership, and Ethical Lawyering
March 2 - 4, 2020
Capital Hilton
Washington, District of Columbia

Join the National Attorneys General Training and Research Institute (NAGTRI) for the inaugural NAGTRI Academy. By bringing together state and territory assistant attorneys general, federal, state, and local government officials, and law students from across the country to explore ethical and moral dimensions of leadership and lawyering, NAGTRI Academy will expand the understanding and promote the crucial importance of ethical conduct and civility in the government legal community.

This unique three-day training will provide members of the government legal community with insights and real-world applications on the topics of:

- Civility
- Communications
- Conflicts of Interest
- Ethics
- Leadership
- Navigating Interpersonal Conflict
- Working with Partners

This three-day Academy is open to all attorneys in attorney general offices, with a programming focus for line attorneys and mid-level managers.


Paid registration will open in January 2020.
FIGHTING CORRUPTION THROUGH INTERNATIONAL COOPERATION

GINA CABREJO, NAGTRI CRIMINAL JUSTICE INSTRUCTOR, LATIN AMERICAN PROGRAMS, NAGTRI CENTER FOR INTERNATIONAL PARTNERSHIPS AND STRATEGIC COLLABORATION

A “thorn in one’s side” is “a source of continual annoyance or trouble.” Corruption in Latin American countries has become the thorn in their side: the difficult-to-eliminate problem for Latin American governments working against corrupt actors. It can sometimes seem that the corrupt side is winning the battle against the transparency sought by the governments. Huge corruption scandals are a common feature in the newspapers and television news; citizens are becoming weary of paying increasingly expensive taxes that go straight to the pockets of corrupt individuals, and this situation gives rise to strikes and protests against the government, as well as individual and collective public complaints. Although the overall picture in many countries looks dark, international cooperation has been a key in the fight against corruption.

Public corruption is generally understood to involve a breach of public trust and/or abuse of position by government officials and their private sector accomplices. Typically, it occurs when a government official asks for or accepts anything of value (whether pecuniary or some other advantage) in return for being influenced in the performance of their duty. Public corruption involves both government officials or employees and their private sector accomplices who offer the thing of value.

One of the biggest corruption scandals in Latin American countries is the “Car Wash case,” also known as Lava Jato or the Odebrecht case. This case, prosecution of which is ongoing, has led to new avenues for international cooperation against corruption and provides an excellent example of why international cooperation is key in efforts to investigate and stop public corruption.

Odebrecht S.A. started in 1944 as a small family construction group, founded by Brazilians in Salvador de Bahia and Sao Paulo. The company grew very fast and now operates in the Americas, the Caribbean, Africa, Europe, and the Middle East. Odebrecht has a diversified business in the construction industry and in the development and operation of infrastructure and energy projects. It also does business in the fields of chemicals and petrochemicals, mining, offshore oil, and gas rigs. Odebrecht has constructed power plants, railroads, ports, and airports in different countries throughout the world.

The corruption case involving former employees of Odebrecht began in Brazil, with a small investigation called Operation Car Wash (in Portuguese “Operação Lava Jato”). The first accusation was made in 2008 by a businessman who reported an attempt to launder money through his company. The police wiretapped the phones of a transfer business housed in a building that had once housed a car wash. This money-laundering investigation led to allegations of corruption at Petrobras, the Brazilian government-owned oil company headquartered in Rio de Janeiro. Petrobras executives deliberately overpaid on contracts with various companies for office construction, drilling rigs, refineries, and exploration vessels. The contractors were guaranteed business on very advantageous terms if they agreed to divert a share of every deal into secret slush funds, which were used for the personal gain of the participants and to finance campaigns of politicians.

Although many companies throughout the Brazilian economy participated in the scheme, Odebrecht’s involvement was particularly extensive and sophisticated. The investigation revealed that Odebrecht created an entire fraud division, known as the Division of Structured Operations. The Division was a secret financial structure with dedicated employees, computers, and off-book communications systems that allowed the co-conspirators to communicate with each other via secure emails using codenames and passwords. The structure had a series of offshore entities that were not included in the balance sheets and, for many years, had a chief of the division reporting to the highest level within Odebrecht. Bribes were approved and paid via wire transfers, using shell companies and a complex network including offshore bank accounts and off-book transactions. The operation was also
run through foreign banks and corporations, some of which were in the United States, which were used to hold and disburse these unrecorded funds. The chief executive officer of Odebrecht was convicted of paying more than $30 million in bribes and was sentenced to 19 years in prison. So far, the investigation has uncovered bribes of more than $750 million, allegedly paid to government officials and political parties in 12 countries.

Currently, the Car Wash case is being investigated by the United States Department of Justice, Brazil, and nine other Latin American countries. The Brazilian federal prosecution office and the financial intelligence unit in Brazil worked closely with the United States and Switzerland throughout this investigation. United States involvement in this case is due to meetings held in Miami by two Odebrecht employees with co-conspirators to advance the scheme. In addition, some of the offshore entities used by Odebrecht operated in the United States.

For anyone involved in anti-corruption efforts, it is remarkable (and instructive) to see a scheme of this magnitude. The overall structure and operation demonstrate how ingenious and well-organized the perpetrators were.

It is also heartening to see how international cooperation among Latin American countries and between Latin American countries and the United States has led to positive results in the fight against transnational corruption. Without international collaboration and agreements, the investigation and prosecution might have ended far sooner and been far less successful.

International cooperation on complex criminal matters may occur in several ways. The most formal agreements on prosecutorial cooperation are treaties, and most countries in Latin America have signed the Inter-American Convention on Mutual Legal Assistance of the Organization of American States. This agreement contemplates assistance in a variety of areas, including notification of rulings and judgments; taking of testimony or statements from persons; immobilization and sequestration of property, freezing of assets, and assistance in procedures related to seizures; searches or seizures; service of judicial documents and transmittal of documents, reports, information, and evidence.
Other important international efforts include the Lima Commitment, which promotes the exchange of information and evidence and coordination in the investigation and prosecution of transnational crimes. It was signed by 34 countries at the Eighth Summit of the Americas held in April 2018 in Lima, Peru. The Lima Commitment reaffirms the intent of the signatory nations to fight against corruption through the applicability of international treaties such as the United Nations Convention against Corruption (UNCAC) and the Interamerican Convention against Corruption (IACAC). In addition, it emphasizes strengthening democratic institutions and the rule of law by increasing government transparency and promoting stronger anti-corruption laws. This commitment is very significant because it is the first time in history that the hemisphere’s countries approved a commitment against corruption. Its impact continues to grow, and the agreement is attracting the interest of international organizations. In September 2018, the Organization of American States (OAS) and the international organization of the Joint Summit Working Group (JSWG) signed an agreement to support the Lima Commitment through technical, political, and financial resources.

Mutual Legal Assistance Treaties (MLATs) are the most frequently used tool in prosecutorial cooperation. MLATs are bi-lateral agreements that allow generally for the exchange of evidence and information in criminal and related matters. They can be extremely useful as a means of obtaining banking and other financial records from treaty partners. The United States has executed MLATs with Argentina, Brazil, Uruguay, and Venezuela, and has signed, but not yet brought into force, a mutual legal assistance agreement with Colombia.

Each MLAT is unique, but, generally, when a request is made through an MLAT, it includes background information about who is investigating whom and for what charge, enough information about the facts of the case for the foreign authority to conclude that a crime has been committed and to see the relevance of the evidence that is being sought, the precise assistance requested, and the text of the statutes alleged to have been violated. When a request is made under an MLAT, it is made directly from the U.S. Department of Justice to the central authority designated in the treaty. Although MLATs are extremely important tools, the process takes time, which is of concern to prosecutors worldwide. Constraints in various countries on sophisticated forensic and financial analysis, legal limitations on ways of gathering evidence, and court congestion are some of the factors creating delays. Nonetheless, the MLAT process has been a large step forward in international anti-corruption efforts.

Other bilateral treaties also may include legal assistance provisions. Latin American countries have made significant advances in international cooperation with the signing of important bilateral treaties that facilitate obtaining banking and other financial records from a treaty partner. For example, in 2018, Brazil and Argenti-
na signed an agreement to share evidence. The Brasilia Declaration for International Judiciary Cooperation, signed by several countries including Argentina, Brazil, Colombia, Chile, Dominican Republic, Ecuador, Mexico, Panama, and Venezuela, permits additional cross-jurisdictional cooperation in the fight against bribery, money laundering, and public corruption.

On a somewhat less formal level, the U.S. Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN) has a memorandum of understanding (MOU) or an exchange of letters in place with the financial intelligence units (FIUs) of many countries to facilitate the exchange of information between FinCEN and the respective country’s FIU. FinCEN has an MOU or an exchange of letters with the FIUs in Argentina, Brazil, Chile, and Paraguay.

There are, of course, many examples of informal international cooperation between prosecutors. New communications networks allow prosecutors to call a foreign counterpart and ask for financial information. Subsequently, if the information is relevant, the evidence must be requested through an MLAT in order to be admissible at trial. Nevertheless, the initial request between counterparts allows both countries to investigate more quickly and results in more efficient and effective prosecution. This successful technique has been implemented in Latin American countries and the communication network is growing ever wider and more robust. Other informal means of cooperation include taking depositions of voluntary witnesses at embassies or consulates of the investigating country and making police-to-police requests.

Regional cooperation is also occurring in the creation and implementation of compliance programs. Companies are being urged to implement and assess their compliance programs to mitigate fraud and to ensure ethical practices by implementing policies, procedures, and good practices. The benefits of a strong program include not only regulatory and legal compliance but also operational benefits. Effective compliance programs work in tandem with a company’s risk management strategies and the transparency of their internal regulations and procedures. Improved compliance programs will help prevent misconduct by corporate employees before it starts.

As the thorn of corruption continues in Latin America’s side, disrupting trust between citizens and their government, the fight against corruption continues with more force thanks to the international cooperation on prevention, investigation, and prosecution.

Endnotes

4 Id.
Global Cooperative Efforts Required to Prevent Cybercrime

This group was asked to consider and discuss the importance of fostering global cooperation to prevent cybercrime and effective methodologies addressing this issue. They were asked to focus on how prosecutors can work with their international counterparts to ensure successful and strong cybercrime investigations and prosecutions as well as what barriers exist that prevent effective collaboration among international prosecutors. The group offered their recommendations, such as the creation of an internet platform prosecutors working group, an international forum and database for cybercrime prosecutors, and a call for governments to dedicate resources to the institutions that fight cybercrime.

Cybercrime is constantly becoming more sophisticated and neither criminal laws, best practices, nor policies addressing cross-border cybercrime have kept up with it. The territorial and jurisdictional limits of laws can make it more complicated and difficult for investigators and prosecutors to collect data and evidence across borders. Prosecutors, government attorneys, and law enforcement officers must continually adapt to new technologies that criminals are adept at using. Almost all crimes today involve some form of online presence, which means that the importance of fostering global cooperation with effective methodologies to prevent cybercrime has never been greater. Transnational cooperation among prosecutors in different countries is vital to preventing cybercrime and deterring other criminal acts.

The Blue Whale Case

One horrendously tragic case illustrates the dangers of social media and how prosecutors must be part of the conversation to resolve these challenges in an increasingly global society. Forging relationships between police and prosecutors will help in the investigation and prosecution of cybercrime that crosses borders. This case study highlights the dangerous impact cybercriminals have on our society and people worldwide.

The specific case known as the Blue Whale suicide game utilized social media to encourage minors to commit suicide and affected children in various parts of the world. A group administrator was assigned to render daily tasks to group members, which they had to complete over a 50-day period. The tasks were horrendous and included destructive behavior like self-harming, watching horror movies, and waking up at unusual hours. On the 50th day, the controlling manipulators of the social media group reportedly instructed youngsters to then kill themselves.

Moldova was significantly affected by this case—numerous children committed suicide. However, under Moldovan law, it was not clear how the activity should be prosecuted. Improved regulatory action, communication, and collaboration between law enforcement authorities of different countries were necessary. To prevent continued criminal activity and additional suicides, law enforcement forces called upon adults within and outside Moldova
to increase vigilance and awareness of the problem, and the Moldovan Parliament raised the issue of tightening controls over the internet and creating a public institution with special skills in this area. Many trainings were held in schools and universities. Although parents and close relatives were the most important factor in preventing adolescent participation in “death groups” and monitoring their online activities, the extensive efforts in schools were still valuable in raising awareness and preventing additional deaths. These efforts helped make children less apt to feel alone and abandoned by those supposed to protect them.

To supplement these preventative measures taking place in schools and by law enforcement, the Prosecutor General’s Office of the Republic of Moldova (PGO) also took steps to engage with representatives from other Moldovan institutions, such as the Ministry of Internal Affairs, the Ministry of Information Technologies and Communications, and representatives from civil society and private companies. These efforts also included service providers, mobile and fixed operators, mass-media, and non-governmental organizations that specialized in child protection and suicide prevention. These efforts helped make children less apt to feel alone and abandoned by those supposed to protect them.

Although the illustrative case resulted in unfortunate casualties, it inspired recommendations and observations to help facilitate improved coordinated efforts among investigators and prosecutors.

**Challenges in Using the Mutual Legal Assistance Process**

As in the Blue Whale case, prosecutors commonly use the MLAT process, especially in cases with cross border elements. This routinely-used process is available to prosecutors and law enforcement officers who need to obtain evidence and information relating to cybercrime cases from treaty affiliates. MLATs are bi-lateral agreements, and in the United States are processed through the U.S. Department of State and the U.S. Department of Justice. Every country does not have a reciprocal treaty with every other country. For example, with respect to the United States, Algeria, Bermuda, and Columbia do not have an MLAT.

Law enforcement officers around the world report that when it comes to using MLATs to address cybercrime across borders, officers do not know who to contact or to trust and are not sure which language or descriptions to use when requesting information. The officers also report that MLAT requests are not as efficient as they had hoped. Although officers want to use the MLAT process, they are reluctant to do so because the process often is time consuming and will likely delay their investigation.

Reasons for the delays include the requirements that the MLAT process be lawfully conducted and compliant with laws governing the sharing of information between countries. For instance, criminal laws describing probable cause in one country may be very different from the definition of probable cause in the counterpart country. Appropriately, governments balance free speech, privacy rights, and intrusion against the urgent need for critical information. Additionally, law enforcement officers, including prosecutors, need to be properly trained to draft requests that are thorough, accurate, and use appropriate language so that the request is manageable and not overly broad.

This game had a huge impact on Moldovan society, but it also unfortunately affected people from around the world, reaching minors in the Russian Federation, Ukraine, Romania, Brazil, and India. The game resulted in numerous teenagers dying by suicide. Eventually, in November 2016, Philipp Budeikin was held accountable and arrested in the Russian Federation and was charged with inciting teenagers to suicide. At the time of his arrest, he was only 21 years old and ultimately was sentenced to three years imprisonment. This awful case serves as an example of how social media may be used in harmful ways, but it also serves as an excellent illustration of how, through global, collaborative efforts, effective strategies can be employed in holding offenders accountable by sharing information quickly and ultimately saving lives.
In addition to the inconsistency in national laws, there is no current global directory or database to access current contact information for specialists and counterparts around the world to serve as experts both before and during trial or to serve as consultants. There is a dearth of up-to-date training and education for prosecutors to stay abreast of emerging trends in technology, and there are no substantively accurate boilerplate templates for law enforcement officers to use when drafting MLAT requests.

To prevent and prosecute cybercrime, prosecutors and law enforcement officers agree that the highest priority is understanding and working with cutting edge strategies and methodologies. Government agencies often have limited budgets and insufficient funding to stay current with technological advances. One possible solution to increase access to funds would be to identify and solicit grants from other funding sources that will enable prosecutors and law enforcement officials to properly handle their responsibilities. Another option would be for prosecutors and law enforcement to reach out to the research and educational community to help governments keep pace with the quickly changing backdrop of technology.

Prosecutor Internet Platform Working Group

Prosecutors around the world consistently encounter the same fundamental issues when trying to obtain evidence from operators of large, multinational internet platforms. Platform operators routinely decline to publicly disclose the type of data they maintain, the form in which it is maintained, how long it has been maintained, or what data they will provide to investigators or prosecutors. Operators often are slow to respond to requests for data and typically provide little information regarding how long a response will take, if they respond at all.

One potential way to address these issues is the formation of an international working group to represent the interests of prosecutors to the operators of large, multinational internet platforms. The working group could be housed within an established international law enforcement organization and would be composed of representatives from prosecutors around the world. It would be tasked with gathering information from global prosecutors regarding common issues they face and interfacing with platform operators to work towards viable solutions. For example, a working group could push platform operators to create portals for law enforcement that would provide a central repository of information describing how the company handles requests for data, allow prosecutors to submit requests for data, and track the progress of prosecutors’ requests. Although there may be sensitive information that prosecutors or internet platform companies are unwilling to share in this global sphere, it is important to consider creative solutions and start somewhere to address this very problematic issue of obtaining necessary evidentiary information.

A working group could also serve as a means of preventing cybercrime. It would enable prosecutors to unify around common public safety issues and pressure businesses to make changes to their platforms. Prosecutors may, for example, identify a dangerous social media campaign—such as the Blue Whale campaign—and push social media networks to identify and remove related content, or push social media networks to help secure users’ information by turning certain privacy settings on by default.

This type of effort has had success in the recent past. In 2013, in response to a rapid rise in smartphone theft, prosecutors, police, and political officials from the United States and England formed a coalition calling on smartphone manufacturers and software providers to make changes to their products to deter theft. Industry responded, and within the next year Apple, Samsung, Google, and Microsoft introduced a “kill switch,” which enabled cell phones to be disabled remotely. Smartphone theft declined “dramatically” in a single year where the “number of smartphones stolen dropped by 50% in London, 27% in San Francisco and 16% in New York.”

New Legislation and Training

A key issue affecting prosecutors’ ability to enhance global cooperation in preventing and fighting cybercrime is the lack of substantive legislation. Prosecutors and law enforcement agencies around the globe should combine all efforts and apply pressure to implement specific national and international regulations addressing the following topics:

1. Facilitating and expediting mutual legal assistance and cooperation
2. Obligating Internet Service Providers (ISPs) and other tech companies to appoint national and international points of contact
THE BLUE WHALE SOCIAL MEDIA APP HAD SERIOUS CONSEQUENCES AND LARGELY IMPACTED MOLDOVAN SOCIETY AND THE REST OF THE WORLD. PROSECUTORS REliED ON THE MLAT PROCESS TO COLLABORATE WITH INTERNATIONAL LAW ENFORCEMENT AND SENTENCE THE PERPETRATOR.

3. Arranging for faster access to online data when seeking evidence

4. Enacting specific criminal provisions related to cybercrime, and

5. Adapting existing criminal procedures and investigative measures to tackle new types of cybercrime

Creating an international forum and database where designated prosecutors from different countries work on strengthening existing laws and methods and drafting new legislative models would be a major step toward improving the legislative landscape. An existing forum and database that could be used for this purpose is the Global Prosecutors E-crime Network (GPEN), a forum of the International Association of Prosecutors (IAP). This existing network brings together global prosecutors to work on common issues to protect consumers against fraud and other criminal activity, including those committed using the internet.

The call for new cybercrime legislation in each country would certainly be stronger and more convincing if prosecutors could easily point to existing laws and mechanisms in other countries that seem to have resulted in successful prosecutorial outcomes. Examples include new procedural rules to force a suspect to assist in unlocking electronic devices; laws that allow access to online data from a suspect’s device in the country of jurisdiction no matter where the data is actually stored; laws that define new elements of cybercrime; and the exploration of technical and legal aspects of accessing data recorded by artificial intelligence tools like Alexa or Siri.

Another important step to enhance global cooperation is holding more international exchanges and conferences as well as training courses. If investigators and prosecutors have access to cutting edge material and techniques, in addition to having a better understanding of cybercrime, possible investigative measures, and varying international legal systems, they will be able to improve their prosecutions and work proactively to prevent cybercrime. The key to more effective and successful cooperative efforts includes developing personal relationships and building connections among prosecutors throughout the world.
The international community should provide more funding for international conferences and seminars that may be organized by global or national authorities and organizations. Those meetings should include programs like those offered by the National Attorneys General Training and Research Institute and the IAP.

More Resources

Effective implementation of any measures meant to combat cybercrime requires that adequate resources be made available. Whereas, some developed countries like the United States and the United Kingdom have committed significant human and financial resources to fight cybercrime, many developing countries in Africa, Asia, Europe, and Latin America have been unable or unwilling to prioritize cybercrime prosecution and commit resources. The transnational nature of cybercrime means that perpetrators are committing crimes across territories and borders, and each government needs to devote adequate resources to law enforcement agencies to counter these cybercriminals.

There are clear disparities in the knowledge levels and available resources among law enforcement agents, prosecutors, and judicial officers. Accordingly, governmental resources should be available to promote uniformity in training and offer training opportunities for the least knowledgeable practitioners. Adequate financial resources also will allow law enforcement agencies to obtain current technological tools and equipment as well as give them the ability to invest in information technology (IT) tools that counter the ever-growing cybercrime wave.

Countries are not similarly situated in terms of available financial means, priorities, and capabilities, but all countries can contribute significantly in other demonstrable ways. In order to overcome the existing resource challenges, countries should consider undertaking the following measures to bridge their resource gaps:

1. Make it a government priority to finance criminal justice initiatives that fight cybercrime.

2. Invest in public-private partnerships to train practitioners, develop IT tools, and make provisions to acquire technical equipment.

3. Improve communication, coordination, and cooperation among law enforcement agents and relevant institutions. Informal channels will especially help countries to cut down on associated costs of investigating and prosecuting these crimes.

4. Commit to recovering assets and confiscating proceeds derived from cybercrime. These recovered assets can in turn be obligated to special funds created for the purpose of continuing to address cybercrime issues, such as training and improved investigations and prosecution efforts.

Conclusion

The challenges of combating global cybercrime are not insurmountable. It just takes sincere commitment. Fostering greater cooperation among international prosecutors can be achieved through a few effective methods, including developing and using informal lines of communication, creating an internet platform working group and an international forum where cybercrime prosecutors can collaborate, and increasing funding from governments or public-private partnerships for IT and international training. Each of these measures would go a long way to address the global problem of cybercrime.

Endnotes

This group was asked to consider and discuss the importance of overcoming hurdles to secure evidence from social media companies and offers some recommendations to help reduce cybercrime, with an emphasis on how international prosecutors can work together and with social media companies to make the evidence gathering process more efficient for both parties.

Primary Hurdles Facing Prosecutors Obtaining Evidence

For prosecutors, there are several barriers to efficient access to data-based evidence from social media companies. Investigators and ultimately prosecutors cannot properly litigate and prosecute cases because they often cannot obtain vital evidence to prove their cases. Or, they cannot receive the evidence quickly enough, further hindering their ability to efficiently and effectively handle their cases. Other obstacles include:

1. Difficulty securing responses from social media companies located outside of a country’s jurisdiction. Unfortunately, prosecutors are treated differently with respect to their ability to access information depending upon their regional location. Prosecutors
in the United States and prosecutors from countries around the world are not similarly situated for a variety of reasons. While the Mutual Legal Assistance Treaty (MLAT) was designed to solve the problem of extra-territorial evidence collection, its effectiveness is extremely limited when prosecutors and investigators seek evidence from social media companies or try to obtain other electronic evidence.

2. Lack of knowledge of the primary point of contact at social media companies and what data they retain. Prosecutors also need to know what terminology must be included in their requests to guarantee a complete response. Their requests must carefully balance both privacy of users and resource considerations.

3. Uneven responses to legal process from social media companies. The companies regularly provide notification to subscribers and suspects of investigative requests, while not providing quick or thorough responses to prosecutors or investigators. Although some companies are responsive to requests, others ignore them or make the process of obtaining information and evidence exceedingly difficult, even in instances where there are exigent circumstances.

4. Social media companies overburdened by the increase in requests from law enforcement around the world. The exponential increase in volume results in many companies being even less responsive or less timely, if they respond at all.

5. A lack of uniform international law or standards concerning how to and whether there are viable options to access information from social media companies. These global inconsistencies in practice and in law have resulted in different data retention periods for different countries (if such requirements are imposed at all). This is a major challenge for prosecutors and investigators because if a crime is not discovered for some time, by the time the request for information is made, the evidence may have already been removed or it may not have been retained in the first place.

6. Encrypted apps and devices. Investigators and prosecutors have been gravely affected by encrypted data on some social media platforms that makes retrieval of evidence all but impossible. Lives have been jeopardized or even lost as a result of the inability to access encrypted materials from social media platforms.

7. Different evidentiary standards. Evidentiary standards in the United States are often different from those in other countries. Often, when global prosecutors seek information from U.S.-based companies or countries using the MLAT process, it is of no use because countries must first meet the U.S. probable cause requirement. This requirement is not a part of the legal process in many countries, which makes MLATs with the United States far less useful.

**Recommendations**

Overcoming the previously noted hurdles will not be an easy feat for international prosecutors or their governments. Social media companies have cited their privacy and their users’ privacy rights as a reason for declining to cooperate with law enforcement officials in investigations. While not all these assertions may be made in good faith, it is certainly understandable that companies want to protect their businesses from intrusive foreign government interference, although they recognize an obligation to prevent their platforms from being used to further criminal enterprises. The following recommendations may be difficult to implement, but they are purposely basic, so that they can be implemented as first steps to encourage companies to be more responsive to prosecutorial requests made for legitimate governmental purposes.

In summary, we recommend the following principles:

1. Widespread adoption of an international framework for cybercrime cases that focuses on improving the effectiveness of the MLAT process.

2. Significant increases in training for law enforcement who work on social media cases to help them operate on a more level playing field.

3. Insistence by governments and society at large that social media companies make efforts to accommodate law enforcement requests where possible.

In addition to these general recommendations, we include some more specific recommendations to help resolve challenges prosecutors face when attempting to obtain evidentiary information from social media companies.
Fully Utilize and Adopt the Budapest Convention

The Council of Europe Convention on Cybercrime, known as the Budapest Convention (the Convention), is a significant tool that should be more widely adopted among nations committed to preventing and minimizing the effects of cybercrime. The Convention is the first multilateral treaty on crimes committed via the internet and other computer networks. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation. Signatories to the Convention are currently negotiating an additional protocol on accessing data in the cloud, which will help facilitate better access to social media and cloud-based evidence in the future. Diplomatic efforts should be used to persuade non-participating countries that have not taken a strong stance against fighting cybercrime to join in the fight and use viable treaties that help alleviate the problem. Widespread adoption and implementation of the Convention should be encouraged at the highest levels of government. With additional support from more nations, it will become more effective.

Improve the Effectiveness of the Mutual Legal Assistance Treaty

Law enforcement officials use the MLAT mechanism to obtain information and fulfill legal requests among participating nations. Unfortunately, the effectiveness of this process can be significantly delayed for a variety of reasons, including countries refusing to respond or responding very slowly, requests being inadequately prepared, or legal standards involving privacy and compliance with existing laws preventing or limiting a response. However, even in instances where all requests are legally sufficient and adequate, MLAT requests simply do not receive a prompt response and are therefore unhelpful. This process must be improved so countries can obtain admissible evidence on criminal matters across borders.

Addressing the following issues will make the MLAT process more efficient and effective:

1. Due to exponential growth in requests for evidence held by social media companies across borders, the number of attorneys who are authorized to handle MLAT requests in participating MLAT countries should be increased.

2. Where possible, the process should be streamlined to ensure that prosecutors are aware of necessary legal requirements for MLAT requests in the requesting country so that response time is improved.

3. Improving transparency of the MLAT process so that law enforcement and justice agencies have greater insight into the status of a request and what can be done to expedite it is important. For example, knowing whether a request has been accepted, is pending or denied, or whether it has been transferred to the domestic authority for action is very helpful to the requesting entity. We encourage the development of an e-MLAT portal to facilitate greater transparency and speedy action in processing requests. Although implementation of an e-MLAT portal may cause concern with respect to sensitive information being shared, given the urgent nature of the requests, it is essential to modernize the process.

4. Use more informal cooperation mechanisms to more precisely identify the parameters for formal MLAT requests, including whether the data is available or would be useful as evidence. These steps should reduce the overall need for and number of MLAT requests. Bringing together professionals and developing relationships, as is done through NAGTRI's International Fellows Program, is a great way to build trust and ensure that prosecutors are more responsive when these requests arise.

5. Consider whether the model of facilitating MLAT requests adopted by the European Union’s Judicial Cooperation Unit (EUROJUST) or the Budapest Convention’s 24/7 network would be useful to expand globally. Through these types of programs, prosecutors would have a contact point in each country to determine whether there is a similar investigation within a country and to help coordinate resources.

6. Encourage the negotiation and adoption of agreements envisioned by the Clarifying Lawful Overseas Use of Data Act, that enable law enforcement and prosecution agencies to more directly access data held by social media companies.
International prosecutors face a variety of obstacles when attempting to collect evidence of a crime from social media companies.

Improve Communication and Relationships Between Law Enforcement and Social Media Stakeholders

It is an understatement that law enforcement officials and social media companies have not been able to maintain a very fruitful relationship. Although some social media companies and law enforcement officials have solid relationships that have been built over the course of time, these seem to be few and far between. The importance of wide-ranging efforts to improve relationships and communication on both sides cannot be overstated. We believe the following steps should be taken to improve communication and enhance relationships among social media companies, law enforcement, and justice agencies:

1. Encourage regular communication among social media companies, law enforcement, and justice agencies to build relationships and trust, ultimately improving each other’s expectations and leading to better cooperation.

2. It is in the interest of social media companies to build and sustain digital ecologies free from crime, in order to create safe spaces for citizens to participate. Therefore, fostering common points of interest between social media companies and law enforcement or justice agencies will help facilitate safer spaces and diminish the illicit corners of the web.

3. Currently, warrants to obtain data from social media companies tend to be broadly framed to ensure that all relevant data is captured. Generally, large volumes of data are returned, which intrudes on users’ privacy, is costly, and can tie up valuable law enforcement and prosecutorial resources when sifting through vast amounts of data. It would be better to have a clearer understanding of the types of data held by social media companies so that search warrants can be more precisely drafted and only requested data is provided.

4. Knowledge sharing among law enforcement and prosecutors is critical because government officials throughout the world are not similarly situated. It is critical that best practices and resources be shared globally to help all enforcers keep pace with technological advances.
Increased Training for Law Enforcement in Social Media Investigations

Training is important regardless of the participant’s experience or knowledge level. Training law enforcement (loosely defined as any stakeholders who are essential to solving cybercrime) so they are better equipped with a practical understanding of how to obtain data from social media companies is important. It is equally important that they know how to obtain material more expeditiously.

Law enforcement officials should have training opportunities to keep pace with technological advances. They should receive training on which tools should be used for different requests, how those tools differ, how data is processed, and how to make appropriate requests to social media companies. Some examples of resources include the following websites or materials:

- Using an online database to access information and obtain possible legal points of contact to assist with elements of investigation and prosecutions at [https://www.search.org/resources/isp-list/](https://www.search.org/resources/isp-list/)
- The [FBI National Domestic Communications Assistance Center](https://www.fbi.gov/services/cjis/national-dominic-comms-assistance-center)
- The [Council of Europe Resources to Combat Cybercrime and Implement the Convention](https://www.coe.int/en/web/cybercrime)

Prosecutors should also be using the best tools to process and utilize electronic evidence, including the International Association of Prosecutors and the Digital DA (for U.S. prosecutors only). Development of similar sources worldwide should be a priority.

Social Media Companies Should Streamline Law Enforcement Requests

Currently, each social media company has individual requirements with which law enforcement and justice agencies must comply in order to obtain electronic evidence. Complying with these individual requirements takes time, and technical non-compliance can be a basis for refusing requests. We recommend streamlining and harmonizing the process by which requests are made, as well as the way in which data is provided to allow easier searches of data by prosecutors. Simplifying the process and information will help prosecutors to work more efficiently.

Conclusion

We recognize that implementing these recommendations globally is not an easy feat, presenting challenges such as how to balance the important privacy interests of users, the business interests of social media companies, and the needs of law enforcement and justice agencies to investigate and successfully prosecute crimes. Protection of the public is a compelling reason to work towards improving the process.

Endnotes

This group was asked to ponder the conundrum that prosecutors often face where they respond reactively to fraudulent internet activity after becoming aware of cases when investigators or non-governmental organizations alert them. They were asked to focus on ways in which prosecutors may take a more proactive role in developing strategies that help minimize the impact or prevent altogether cybercrime scams, fraudulent activity, and harassment of vulnerable groups and the public in general. The group identified the most vulnerable populations, challenges for these groups and law enforcement, highlighting the participants’ country-specific scenarios, and offered their recommendations for lessening the effect of cybercrime on these individuals.

As cybercrime becomes more lucrative, widespread, and easy to commit, all citizens are at risk for victimization by criminals using social media. However, vulnerable populations are most at risk and severely affected by social media scams and frauds. These vulnerable populations across the world typically include the elderly, victims of intimate partner violence, minor children, immigrants, and the unemployed. Prosecutors should identify these groups as well as regionally-specific vulnerable populations in their jurisdictions to better protect them through education, communication with law enforcement, and prevention techniques. This article identifies the most vulnerable populations and their challenges, and offers suggestions and recommendations on how best to prevent them from becoming victims of fraudulent uses of social media.

Identifying Vulnerable Populations

The most vulnerable members of society when it comes to cybercrime are often those who trust easily, tend to be more naive, and are less adept with the ever-advancing world of technology. Efforts to prevent cybercrime should identify these likely victims. This process should include analyzing current victim databases, communicating with credit card companies to identify patterns in victim demographics, and partnering with internet payment companies like PayPal to gather information about those filing complaints. Engaging private sector companies in dialogues and encouraging the creation and implementation of law enforcement portals for reporting could aid this data gathering. This process should also include civic groups, such as senior citizen centers and youth organizations, that can best communicate with their members to help protect them.

Across the globe, certain populations are always high-risk targets for cybercriminals. The elderly, those referred to in Ghana, for instance, as “BBC” (born before computers), often lack an innate understanding of technology and social media and are more liable to trust strangers. These citizens are also the most frequently targeted by technical support scams and will provide their personal identifying information and passwords to criminals freely in order to “fix” software accounts which are reportedly “broken.”
Conversely, children and teenagers who grew up using the Internet are so accustomed to sharing the most private information on social media that they fail to consider the ramifications of posting this sensitive material on public forums. Cyberbullying on social media has become rampant, as children use the anonymity of a screen to create fraudulent accounts and harass their classmates. Sexually explicit images of children, both provided willingly and through cases of “sextortion,” can then enter into the larger network of child exploitation content, revictimizing these children every time the files are shared. Both of these groups, in different ways, are more vulnerable due to their more trusting nature.

Other groups are targeted based upon their lack of knowledge regarding financial decision making. Immigrants often arrive in countries unaware of the culture and infrastructure of their new home country, leaving them without a grasp of the language, culture, or financial practices. For example, immigrants may be targeted by scammers via Facebook for assistance in finding homes and/or employment in their new country. Individuals seeking romantic relationships can also be targeted through their lack of understanding in this field. This population, often desperate for connection, are more willing to provide money to perceived romantic partners in order to meet “in real life” and pursue a relationship.

Around the world, there are specific groups that are more directly targeted in specific countries than in the rest of the world. For example, in South Korea, criminals frequently target individuals seeking jobs by requiring that they pay a nominal fee for help in finding a job. These young, desperate job seekers will provide the criminal with bank account numbers, and the criminal will then empty the bank account and disappear, having provided no services to the job seeker. Certain areas of the United States also are more likely to have a high concentration of immigrants, thus resulting in similar predatory activity based upon perceived or actual vulnerabilities. Prosecutors must therefore keep track of local communities to identify the most vulnerable in each area, as well as protecting the typically vulnerable groups.

### Challenges Presented for Vulnerable Populations

#### Social Media

The breadth and magnitude of data shared on social media is staggering. Facebook reports that 300 million pictures are shared on the platform every day, and 510 million comments are posted every minute. Twitter reports that 500 million tweets are posted every day. Facebook reports that 500 hours of video are posted to YouTube every minute. Seventy-five percent of the global population is on some form of social media, and seventy percent of Americans use social media at least once per day.

These private companies have legal and oversight departments that attempt to monitor the behavior of users through artificial intelligence, human review, and other methods. However, with such an incredibly large amount of data being shared on the platforms, these departments cannot see or closely monitor and regulate everything that happens between users. With such a strong focus on the prevention of high-profile crime, such as terrorism, human trafficking, and child exploitation, the more subtle language of social media scammers may go undetected until it is too late. By the time these fraudulent accounts or posts are reported, the victims often have already suffered monetary or emotional harm.

#### Working Relationships

Efficient information sharing processes between internet service providers, social media companies, tech companies, and law enforcement is often lacking, which can be a roadblock to effective working relationships. Legal process differs across jurisdictions and, even with United States law enforcement, it can be labor-intensive to obtain useful data from companies seeking to protect the privacy interests of their users and limit their own liability for sharing this information. Other organizations with a vested interest in these issues, such as child advocacy groups, consulates (in the case of immigrants), and civic groups such as educational administrators and senior centers, are not often included in discussions about social media crime. If the interests of the most vulnerable groups are not represented during the crafting of solutions, they will receive less support and assistance.
Language and Cultural Barriers

Certain groups, based on their own cultural preferences and/or language comprehension difficulties, are less likely to engage with law enforcement when they are victimized. This can be due to a distrust of the police or a cultural norm indicating that the police should not be included in “private” matters. There is also an element of embarrassment, particularly for the elderly, who think they should have known better than to trust the scammer or the person who has exhausted their savings in the pursuit of a perceived romantic relationship.

Working Across Borders

With regard to working across borders with social media companies, the Mutual Legal Assistance Treaty (MLAT) often does not provide prompt assistance to foreign law enforcement conducting investigations. While in theory the MLAT process should provide information to those overseas as easily as those in the same countries as the social media companies, this often is not the case.

Criminals themselves often also reach across national borders to find victims and to avoid detection and apprehension. For example, in Ghana, scammers target older women in the Western world on dating websites such as Badoo.com and eHarmony. The scammers gain the trust of these women and eventually request money for their “weddings,” knowing these women have a pension and therefore have money to help facilitate and fund the scam unknowingly.

Recommendations

Education and Outreach

Law enforcement and community organizations alike should interface frequently with these most vulnerable populations and craft education and outreach programs most likely to resonate with those groups. In Louisiana, for instance, the “Know More Louisiana” program conducts live presentations in schools to inform children of the dangers of cyberbullying and provide them with tools to aid them in combatting the detrimental emotional effects of cyberbullying. In New Jersey, a holiday season awareness campaign set up tables outside technology stores in shopping malls and provided parents with information about protecting their children from potential dangers of their newly acquired tech gifts.

Law Enforcement Methods

Communication is key in creating trust relationships between law enforcement and vulnerable populations. Diversifying the police force will encourage all citizens to see themselves in the faces of law enforcement and encourage wider reporting. Furthermore, law enforcement should receive social media training to better patrol for fraudulent uses and be aware of the populations most at risk for cybercrime. Creating a friendly, open environment and conducting public forums at youth centers will encourage sharing and reporting by these at-risk citizens.

Children often do not have experience with police interactions, and law enforcement should take special care in building relationships with youth. For instance, Israel has a police hotline for children and their parents, which encourages them to call for assistance in protecting themselves online, including guiding them through cyberbullying issues and how to erase unwanted data from their devices. In the United States, a legislative addendum to the Children’s Online Privacy Protection Act (COPPA) increasing the age of a “child” from 13 to 18 would expand these protections to teenagers in some of their most susceptible years. Further training for law enforcement to interact with children in schools and extracurricular activities could inspire trust with the police at an early age as well.

Working with Transnational Partners

Social media companies need to be included in efforts to make their own platforms safer and less susceptible to scams. Law enforcement should be as specific as possible when serving a company with legal process seeking data; however, the company itself should also maintain an open line of communication with law enforcement in order to facilitate the transmission of important evidence with a
Social media platforms routinely store personal data that can aid investigators and governments on matters involving national security and criminal or civil cases.

Proper legal foundation. With the immense amount of personal information shared on social media, companies also should be exercising more care over keeping this data closely guarded, including making all profiles (but especially those of children) private by default.

It is also more important than ever for law enforcement agencies across the world to share information and work together to apprehend cybercriminals. A recent South Korean case involving phishing and fraudulent cryptocurrency exchanges connected South Korean law enforcement officials and the United States Federal Bureau of Investigations, and ultimately uncovered South Korean and Japanese scammers, targeting victims in both of those countries. These agencies used the 24-7 Network, a list of contacts in 50 countries who are available to help with investigations involving electronic evidence, by making efforts to ensure that internet service providers freeze the information sought by a requesting party as soon as possible. They then provided each other with records and evidence based on the Mutual Legal Assistance Treaty. They were able to obtain optimal results by open communication. Law enforcement agencies should maintain open lines of communication and a willingness to assist the larger goal of eliminating social media fraud, even if the case does not originate in their jurisdiction.

Conclusion

There are challenges to preventing social media scams that victimize vulnerable populations. These recommendations seek to facilitate collaboration across nations and improve outreach campaigns that help vulnerable groups protect themselves against scams. This work is not easy and will require consistent efforts and time but, considering the high cost of cybercrime financially and emotionally, these efforts are both worthwhile and necessary. Addressing these issues requires that government officials, including prosecutors, make them a priority, and take a stand to help eradicate this problem. With concerted efforts extended to empower and educate vulnerable populations about the dangers of cybercrime scams and fraudulent activity, predators will find it more difficult to prey on them. Taking such steps, even if incremental in scope, can make a huge difference.

Endnotes

1 James Hale, More Than 500 Hours Of Content Are Now Being Uploaded To YouTube Every Minute, TubeFilter, May 7, 2019, https://www.tubefilter.com/2019/05/07/number-hours-video-uploaded-to-youtube-per-minute/.


4 Budapest Convention on Cybercrime, art.35, E.T.S. No 185 (July 1, 2004).
This group was asked to consider the responsibility that corporations and governments have to ensure protection of private data being stored on social media platforms. These platforms routinely have material stored that will aid investigators and governments on matters involving national security and/or criminal or civil cases. The group discussed the value of personal data and why cybercriminals go to such great lengths to obtain it, the challenges and consequences of failing to protect it, and how to hold entities accountable when they fail to practice good corporate governance or comply with investigations. The article offers recommendations that law enforcement and corporations can implement collaboratively to decrease cybercrime.

Individuals, corporations, and governments from around the world are increasingly embracing and relying upon digital technologies and are moving more deeply into an ever-evolving digital world. This new and ever-developing environment presents significant challenges because massive amounts of personal data are being collected and shared every day, often without the users’ knowledge or actual consent. Personal data has become a valuable asset for governments and for businesses and its use has developed in every sphere. Individuals sometimes choose to share personal information but are more often than not compelled to do so in order to interface with platforms or to receive government or business services being offered. Corporations and governments thus have a joint responsibility to protect private data. This article will examine the current state of affairs with respect to protecting data and make some recommendations about how to ensure that corporations and government institutions take their role seriously to protect citizens’ personal information.

Value of Personal Data and Responsibility to Protect It

More and more often, citizens are notified of security breaches where their personal information has been compromised, whether it includes credit card companies, health care or insurance companies holding personal information of patients, or retailers. These breaches result in very personal data being stolen or acquired by criminals seeking to do extensive harm and often succeeding in obtaining personal information on consumers.

Personal data, including financial or other identifying information, is extremely valuable to criminals. Cybercriminals can use personal data for a variety of illegal purposes, such as harassment, economic crimes including fraud and theft of intellectual property, or simply a sale of information to advertising and marketing companies for profit. They also can use it to disrupt infrastructures, such as banking systems and health care services. Both...
corporations (who collect and hold information) and govern-
ments (who also collect and hold information but have an additional public interest duty and mandate to protect citizens) have a responsibility in this situation. Both should assist and enable law enforcement to effectively investi-
gate cybercrime and both should take concerted steps to secure their networks, conduct training for staff, and protect consumers’ very personal data.

The extent to which government and social media companies work with law enforcement and cooperate in investigations is an important consideration for prosecutors and investigators in their work to deter and resolve crimes and hold cybercriminals accountable. Both govern-
ments and corporations have to strike a balance between, on the one hand, the protection of individuals’ privacy and information and, on the other hand, the necessary and appropriate release of the same information for law enforcement purposes. Although it is incumbent upon all parties to assist law enforcement and reveal information when necessary to move investigations forward, corporations are often reluctant to reveal information voluntarily as this erodes customer confidence in the confidentiality of their service.

**Protecting Private Data**

Personal data is valuable to corporations for a variety of reasons and protecting that information should be equally important. In some instances, the data itself is the product and has considerable financial value. In other instances, the personal data supports the primary function of the business. Corporations have many legitimate uses for information ranging from the basics of knowing where to deliver products and services and collecting payment for those products and services to more detailed analysis, for example, analyzing customer trends to predict future buying patterns.

Corporations should also have a strong interest in protecting personal information through appropriate business practices. Loss of data can cause direct financial loss to the business itself, can cause significant reputa-
tional damage to the business, and can result in financial penalties in most jurisdictions. Individuals themselves can, of course, be harmed emotionally and financially by the loss of their personal data through identity theft or harm to their reputation.

Access to government services also depends on the robust collection and sharing of personal data, for example, for public purposes that vary as widely as population statistics and planning, administration of benefits, provision of education, collection of taxes, voting, and public safety. Given that citizens are often compelled by law or regulation to provide personal data to their government, govern-
ments have a strong moral and legal obligation to protect that information.

**How to Protect Data and Prevent Cybercrime**

Corporations and governments both have an important role in preventing cybercrime and protecting personal data and cyber infrastructures. Corporations, in particular, should spend more time and money to protect customer data because they are in a financial position to do so, in part because they are reaping financial rewards from consumers providing that private data. The harmful consequences of failing to do so far outweigh the cost.

Corporations, no matter how big or small, should have appropriate security measures in place to prevent data breaches. Not all data is equally sensitive, so this involves a balancing exercise depending on the sensitivity and amount of the information held as well as the resources of the company. Measures as simple as ensuring that software is updated in a timely fashion can help prevent data breaches and cybercrime. Conducting thorough back-
ground checks and putting into place very stringent safe-
guards and practices to ensure that employees do not have access to material unless they need it to perform their duties would help to minimize and prevent hacks and release of private information. Companies also should have policies that ensure mandatory training, compliance, and security checks.

In addition, corporations should report instances of data breaches to an appropriate body within each affected jurisdiction. Some corporations do not report until absolutely required to do so. To remedy this, governments ought to consider legislation requiring timely mandatory reporting. This will enable disruption of the continuing act of data breach, preservation of evidence, swifter investigatory action, and more effective harm mitigation for victims.
DATA BREACHES AND OTHER FRAUDULENT CRIMINAL ACTIVITY ARE GROWING DUE TO THE POPULARITY OF SOCIAL MEDIA. VULNERABLE MEMBERS OF SOCIETY, INCLUDING THOSE WHO ARE LESS FAMILIAR WITH TECHNOLOGY OR TRUST OTHERS EASILY, ARE MORE LIKELY TO BE TARGETED BY CYBERCRIMINALS.

Governments should collaborate to create and enforce effective legislative standards for data protection. Because cybercrime is borderless, international collaboration is essential. By way of example, in 2018 the European Union issued the General Data Protection Regulation (GDPR), which aimed to harmonize data privacy laws across Europe, protect and empower all EU citizens concerning data privacy, and reshape the way organizations across the region approach data privacy. The GDPR’s penalties for data loss have incentivized corporations to protect information and have already motivated them to improve security and information handling.

Ensuring Law Enforcement Effectively Investigates Cybercrime

Corporations and governments have the responsibility to ensure that law enforcement can effectively investigate cybercrime through suitable legal process. That legal process must of course be consistent with the rights of individuals and corporations. Law enforcement can effectively overcome challenges to investigating cybercrime through legal process (subpoena, court order, search warrant, etc.).

One of the greatest challenges to effective investigation of cybercrime is the stark difference in knowledge about technological capabilities and limitations between the corporate world in general and law enforcement. Corporations are subject matter experts about their systems and best understand their own system capabilities and limitations. Moreover, capabilities and limitations vary widely among corporations. Law enforcement officials are largely dependent on the corporation from whom they are seeking information.

Another very significant problem is that data can be compartmentalized and stored in various jurisdictions. Because cybercrime is transnational, investigating and obtaining digital evidence for cases becomes far more complex and investigations may be stymied when legal process crosses jurisdictions. Currently, access to that data is often dependent upon the Mutual Legal Assistance Treaty (MLAT) process which can be slow, cumbersome, and often opaque to the requesting party. Governments should consider implementing alternative and more prompt ways to share electronic evidence with trusted partners and work towards building trusting relationships where they do not yet exist. Further, governments should also consider ensuring that law enforcement can obtain and use data evidence when it is directly accessible in its
own jurisdiction regardless of where it is stored. In other words, if a case has originated in a European country but the information is available on a server in the United States, the U.S. should ensure that the European country gets the evidence it needs so long as the case has legal merit and meets necessary legal standards. There should never be a delay in obtaining evidence simply because the server or information is not physically in that country of origin.

Governments and nations must work together to ensure that protecting the public safety is the paramount concern. The Clarifying Lawful Overseas Use of Data Act,\(^1\) enacted in the United States in 2018, is just one example of how a government initiative to address territorial jurisdiction issues has helped law enforcement obtain electronic data for evidentiary purposes.

**Recommendations**

The challenges identified above are complicated and there are no easy solutions, but we suggest focusing on two areas that we think will improve law enforcement’s ability to obtain information, protect cases, and protect consumer data that corporations and governments may have. Both recommendations require compromise and commitment but are not too difficult to implement. We understand that lack of trust is an impeding factor that may prevent corporations and governments from working together, but we encourage cooperation to jointly address any challenges that jeopardize consumer data and impede investigations.

One of the most obvious yet challenging solutions to improve corporate and government responsibility is to promote and facilitate improved collaboration. To ensure law enforcement requests are properly focused, the corporation and law enforcement should work collaboratively to identify the capabilities and limitations of the corporation’s systems and the data it has. This commitment to collaborate will both encourage rapid compliance and prevent overly broad disclosures of information.

A second way to improve collaboration is greater use of public-private initiatives. Task forces involving both law enforcement agencies and technology corporations sharing information would benefit both groups. While some issues would have to be addressed in terms of what and how much information is shared, we already have examples where such efforts have been impactful and helpful. The task force model has been particularly effective in financial crime investigations, such as the Financial Crimes Enforcement Network in the United States and the Joint Money Laundering Intelligence Taskforce in the United Kingdom. Additionally, ensuring that policy issues and the need for legislative change are part of the collaborative conversation will also allow corporations and governments to work together to support appropriate legislative solutions.

Governments should engage in a public information campaign that highlights corporate practices that are detrimental to consumers, whether intentional or unintentional. This campaign should focus on informing consumers about what they need to do to protect their data.

Finally, government efforts should also include working directly with corporations to ensure that they only retain information that is necessary for business purposes. There should be an understanding that the persistent storing of consumers’ information is unwarranted, unless actual permission for that sharing is given by the consumers. Prosecutors should be part of this conversation and, when corporations or governments engage in practices that may put consumers’ private information at risk, consumers should themselves have legal remedies.

**Conclusion**

The corporate and government use of personal data has become an integral part of daily life and a large amount of personal data is collected and shared every day for both legitimate and criminal purposes. Corporations and governments have a joint responsibility to protect private data and cooperate with law enforcement. This can be achieved by collaborative efforts, sharing of information, and strong effective legislative response to the malicious use of private data, as well as outreach campaigns to educate the public on how to protect their data and what harm can occur if data is compromised.

**Endnotes**

ARIZONA

Authority to Sue. The attorney general of Arizona sued the Board of Regents of the state university system, alleging that the Board’s tuition-setting practices violated the Arizona Constitution’s requirement that “the instruction furnished [at the university and all other state educational institutions] . . . be as nearly free as possible.” The attorney general alleged that the Board had violated Arizona statutes by directing the universities in question to offer in-state tuition to students who were not “lawfully present” for purposes of eligibility for in-state tuition, and thus failing to collect monies accruing to the state and causing the illegal payment of public monies.

The Board argued that the claims should be dismissed because, among other reasons, the attorney general lacked authority to initiate the lawsuit under the Arizona Supreme Court’s decision in Ariz. State Land Dep’t v. McFate.¹ In McFate, the Arizona Supreme Court examined A.R.S. § 41-193(A)(2), which provides, “At the direction of the governor or when deemed necessary by the attorney general, [the attorney general may] prosecute and defend any proceeding in a state court other than the supreme court in which the state or an officer thereof is a party or has an interest.” The Arizona Supreme Court interpreted the word “prosecute” in this statutory provision narrowly, and held that the attorney general “may initiate proceedings on behalf of the State . . . but these instances are dependent upon specific statutory grants of power.”

The trial court dismissed the attorney general’s action on the grounds that the attorney general did not have authority to file the suit, and the attorney general appealed. The attorney general argued that an Arizona statute (A.R.S. § 35-212) authorizes the attorney general to “bring an action . . . to . . . [e]njoin the illegal payment of public monies” and “[r]ecover illegally paid public monies.” The court of appeals held that collecting tuition does not constitute a “payment” under A.R.S. § 35-212. Because the complaint did not cite to any other statute providing the attorney general with authority to commence the suit, the court affirmed the district court’s dismissal, applying the McFate reasoning.

In a special concurrence, however, the three appellate judges thoroughly reviewed McFate and urged that it be overruled by the Arizona Supreme Court. The judges stated, “McFate’s interpretation of “prosecute” in A.R.S. § 41-193(A)(2) appears to be flawed. The decision overlooks substantial evidence of the plain meaning of the phrase in 1953 [when the statute was enacted].”

The concurrence analyzed Arizona law before McFate and pointed out, “Common usage before and around the time of the 1953 amendment suggests that the term ‘prosecute’ included civil actions and contemplated both the initiation and the continuation of legal proceedings.” The McFate court acknowledged this, but found policy-based concerns about the role of the attorney general supported a more limited interpretation. The concurring judges concluded with an extensive analysis of decisions and interpretations of the term “prosecute” as used in the statute, and noted, “It is up to the Arizona Supreme Court to determine whether those concerns continue to support McFate’s interpretation and whether legislative acquiescence and stare decisis caution against overruling McFate.” State of Arizona ex rel. Brnovich v. Arizona Board of Regents, No. 1 CA-CV 18-0420 (Ariz. Ct. App. Aug. 20, 2019).
KENTUCKY

Attorney General Qualifications. Kentucky statutes allow any qualified voter to file suit to challenge the bona fides of any candidate in a Kentucky election. Plaintiff filed suit, alleging that a candidate for Kentucky Attorney General did not possess the qualifications required by Kentucky’s constitution and statutes. The candidate was admitted to the Kentucky Bar in October 2011. He subsequently clerked for a federal judge for two years, during which time he was prohibited from the private practice of law. He then practiced law in a firm, became legal counsel to the United States Senate Majority Leader, and returned to private practice before becoming a candidate for attorney general of Kentucky.

The court reviewed a 1937 Kentucky Supreme Court decision that defined “practicing law” as “not limited to the conduct of cases in courts. . . . It embraces the preparation of pleadings, and other papers incident to actions and special proceedings and the management of such actions and proceedings on behalf of clients before judges and courts, . . . the preparation of legal instruments of all kinds, and, in general, all advice to clients. . . .” The Kentucky Supreme Court Rules define the practice of law as “any service rendered involving legal knowledge or legal advice, whether of representation, counsel or advocacy in or out of court . . .” and state “[l]awyers may engage in the practice of law in Kentucky . . . as employees of a United States government agency or department.”

Turning to case law, the court described an unpublished decision about a prior candidate for attorney general who had been state auditor of public accounts, which the plaintiff in that case argued did not qualify as practicing law. The trial court held that the candidate was qualified because he had been licensed to practice law for the requisite eight years. The case was appealed, and the appellate court upheld the trial court, agreeing that the state constitution established a broad standard, which was satisfied by someone who has been licensed to practice law for that time period. The appeals court stated, “The constitution establishes only the broadest qualifications. Evaluation of the character and experience of candidates is left to the electorate.”

The court applied the reasoning of these cases and found that because the candidate would have been a licensed lawyer for more than eight years, he was qualified to run for attorney general. The court also held that the two years as federal law clerk may count toward the eight year requirement in the Kentucky constitution. During both those years and his time as legal counsel in the Senate, his positions involved “service rendered involving legal knowledge or legal advice” as specified in Kentucky Supreme Court Rule 3.020. *Jackson v. Cameron*, No. 19CI-5702 (Ky. Cir. Ct. Jefferson Cty. Oct. 9, 2019)

MARYLAND

Parens Patriae Standing. The Maryland attorney general sued 65 defendants over MTBE contamination of Maryland’s waters, alleging common law tort claims and violations of the state’s environmental statutes. The attorney general sued as parens patriae, as trustee of the state’s natural resources, and under the Maryland environmental statutes. The state sought compensatory and punitive damages, costs for testing and cleanup, and an injunction requiring the defendants to test and treat drinking wells contaminated by MTBE.

In the context of a motion to dismiss, the federal district court discussed the state’s parens patriae standing to bring a trespass claim. In its complaint, the state alleged damages “upon the State’s possessory interest in properties it owns, the possessory interest of its citizens in properties they own which the State asserts here on their behalf in its parens patriae capacity, and the State’s possessory interest as the trustee of the State’s natural water resources.” The defendants argued that the state cannot recover in trespass for the alleged MTBE contamination of properties that it does not exclusively possess, and the state responded that it is suing “both as a quasi-trustee of Maryland’s water resources and as a parens patriae representative of its citizens’ water ownership interests.”

The court stated that the widespread contamination of the state’s waters is an injury that is properly redressed in parens patriae. However, proceeding in parens patriae does not “give the State ‘exclusive possession’ of contaminated properties within its borders—even those it does not own—such that it may recover for trespass to those areas.” The court noted that either the state’s quasi-trustee interest in its natural resources, or its parens patriae authority, could give rise to a public nuisance claim, which would not require exclusive possession. *Maryland v. Exxon Mobil*, 2019 U.S. Dist. LEXIS 150177 (D. Md. Sept. 4, 2019).
MINNESOTA

Attorney General’s Restitution Claims Not Blocked by Draft Settlement with Private Class. After a two-year investigation, the Minnesota Attorney General’s Office in July 2017 filed suit in Minnesota state court against CenturyLink, a telecommunications company, “to enforce Minnesota’s consumer protection laws and its parens patriae authority to vindicate the State’s sovereign and quasi-sovereign interest to protect the economic welfare of Minnesota’s citizens.” A private action covering the same claims was filed in California and the case was transferred to the multidistrict litigation (MDL) court in Minnesota in October 2017.

Plaintiffs’ attorneys notified the court that a tentative settlement had been reached, but no final terms had been agreed to, and the state was not involved in those settlement discussions. In the state’s case, the trial is scheduled to begin in March 2020. In the MDL case, dispositive motions were still pending, the class had not been certified, and no settlement had been presented to the court. Shortly after this, CenturyLink filed a motion seeking to enjoin the attorney general’s “duplicative consumer restitution claims” in the state action. In response, the state sought a continuance of the motion until 30 days after CenturyLink filed for preliminary approval of the settlement. The court granted the state’s motion.

The court found that the state had good cause for a continuance. “Both the State and the Court need to be able to review the specific terms of the proposed settlement agreement in order to cogently argue and decide CenturyLink’s motion for a temporary injunction.” The court noted that courts consider stays of parallel proceedings, particularly “those prosecuted by states on their own behalf,” after motions for approval of the class settlement. There are few exceptions to this rule.

The court held

[T]he State is making the request for a continuance in good faith to enable it to meaningfully respond to the motion for an injunction and to protect its sovereign and quasi-sovereign authority to pursue the procedurally advanced state action and vindicate the interests of the citizens of the State of Minnesota. There is no authority for the proposition that a putative class’s undisclosed, potential settlement justifies interfering with an ongoing, procedurally advanced government enforcement action.

NEW YORK

D.C. Federal Court Does Not Have Jurisdiction Over New York Attorney General. The New York legislature enacted a statute, the TRUST Act, which authorizes the chairpersons of certain committees of the U.S. Congress to request the state tax returns of the President of the United States. The President filed an emergency action against the New York attorney general and tax commissioner as well as the House Ways and Means Committee under the All Writs Act to prevent the disclosure of his tax returns; he also filed suit to block release of his returns to the House of Representatives. The president argued that any request would violate Article I of the Constitution, the Rules of the U.S. House of Representatives, and the First Amendment. The court first addressed the questions of personal jurisdiction and venue over the New York defendants.

The president conceded that the court did not have general jurisdiction over the New York defendants. The D.C. long-arm statute, which is applicable here, authorizes specific jurisdiction “over a person, who acts directly or by an agent, as to a claim for relief arising from” certain contacts that person may have with the forum. Those contacts include transacting business in the District of Columbia, causing tortious injury in the District by an act in the District, or causing tortious injury in the District by an act outside the District if the party either 1) regularly does business there, 2) engaged in any other persistent course of conduct there, or 3) derives substantial revenue from goods used or consumed or services rendered there. Under D.C. Circuit law, the District’s long-arm statute does not apply to states themselves.

The court rejected the president’s argument that corresponding with a congressional committee and sending information to that committee would constitute “transacting business” in the District. The court also noted that the New York Attorney General did not have a role under the statute in responding to a request from Congress. Although the attorney general has engaged in litigation activity in the District, the president’s alleged injury did not arise from that litigation, so it does not provide jurisdiction under the long-arm statute. Nor did the attorney general take an action inside or outside of the District that would cause injury to the president inside the District, even if litigation activity could be characterized as a “persistent course of conduct.”
In dicta, the court noted that “Exercising jurisdiction over New York state officials would also raise state sovereignty and federalism concerns.” The court observed that other courts have been “cautious” when considering whether plaintiffs may bring state officials into federal court in another state to litigate the constitutionality of the original state’s statutes. Such jurisdiction has been held to violate the Due Process clause. *Trump v. Committee on Ways and Means*, No. 1:19-cv-02173 (D.D.C. Nov. 11, 2019).

**OHIO**

**State Cannot Delay Counties’ Opiate Litigation.** The Ohio Attorney General petitioned for a writ of mandamus compelling a district court to dismiss or postpone a consolidated “bellwether” trial in a multidistrict litigation (MDL) brought against manufacturers and distributors of opioids by Ohio counties and municipalities. The attorney general argued that, as a sovereign, the state has sole authority to assert parens patriae claims for harms to its citizens’ health and welfare. The attorney general argued that the counties’ claims went beyond direct injury to the counties and sought more expansive relief that duplicates the relief being sought by the state in its own lawsuits against the same defendants.

The Sixth Circuit noted that the state had not moved to intervene in the MDL proceeding to raise the issues on which it now seeks mandamus. The state argued that it would have then been required to subject itself to federal jurisdiction and pursue its claims in federal, rather than state, court. According to the Sixth Circuit, the Supreme Court will find that a state has waived its constitutional protection only if there is express language to that effect. The court also observed that that state did not object when the counties’ cases were removed and consolidated in the MDL, and that the state has taken some actions in the MDL court, including moving for a protective order and opposing certification of a negotiation class. The parties have “conducted extensive discovery, filed numerous pleadings and, in some cases, reached settlements.” The court declined to enter a writ of mandamus. *In re: National Prescription Opiate Litigation*, No. 19-3827 (6th Cir. Oct. 10, 2019).

**WISCONSIN**

**Attorney General Control of Litigation.** Planned Parenthood sued several Wisconsin officials, including the attorney general, in federal court, alleging that various Wisconsin laws and regulations unnecessarily require the participation of a physician during various stages of abortion services, violating the constitutional rights of both providers and patients. The state defendants denied that these requirements violate plaintiffs’ rights.

The Wisconsin legislature sought to intervene, either as a matter of right or by permission. Their motion was opposed by all parties, and the district court declined to allow their intervention. After determining that there was no statutory basis for intervention as of right (under 28 U.S.C. §2403(b)), the court noted that FRCP 24(a) does recognize a right to intervene when “(1) the motion to intervene is timely filed; (2) the proposed intervenors possess an interest related to the subject matter of the action; (3) disposition of the action threatens to impair that interest; and (4) the named parties inadequately represent that interest.”

In this case, the first element was satisfied. Turning to the question of the intervenor’s interest, the court distinguished between the interest required for Article III standing and that required for intervention in the 7th Circuit. The interest required for intervention must be unique to the proposed intervenor. In this case, the state defendants’ interest—defending the constitutionality of challenged statutes—is the same as that of the legislature.

The court then addressed the third factor, the threat to the intervenor’s interest. The legislature argued that a court decision in favor of the plaintiffs could nullify the “majority votes in support of the challenged measures.” The court cited 7th Circuit precedent that legislators have standing to challenge measures that diminish the effectiveness of their votes, but the decision of a court that a statute is unconstitutional is not nullifying a legislator’s votes. The legislature also argued that “an adverse decision in this case could have an impact on the legislature’s ability to pass abortion-related legislation in the future.” The court observed, “While any decision in this case necessarily will be limited to the challenged regulations, any attempt by the legislature to reenact the same regulations would be thwarted. However, the desire to reenact invalidated legislation hardly serves as a cogent basis for intervening.”
The court then addressed the question of whether the legislature is inadequately represented by the attorney general. Past Seventh Circuit cases have held, "when the representative party is a governmental body charged by law with protecting the interests of the proposed intervenors, the representative is presumed to represent their interests adequately unless there is a showing of gross negligence or bad faith." The court noted that under Wisconsin law, the attorney general "has the duty by statute to defend the constitutionality of state statutes. . . . Nothing about recently-enacted Wis. Stat. §803.09(2) strips the attorney general of that obligation, nor have the proposed intervenors offered evidence that the attorney general does not intend to fulfill this responsibility.

The legislature argued that the attorney general might not litigate the case as ardently as the legislature because, among other things, he received donations from Planned Parenthood during the election, he withdrew Wisconsin from two amicus briefs defending abortion regulations in other states unrelated to the ones at issue here, and he chose to answer the complaint, rather than file a motion to dismiss. The court held "this litany fails to demonstrate (or even come close to demonstrating either gross negligence or bad faith." The court also noted that the same attorneys who defended the regulations under the prior attorney general are also defending this action.

The court also declined to exercise its discretion to allow permissive intervention, for the same reasons described above. The court observed that the legislature could file amicus briefs, could renew its motion to intervene if the attorney general declined to defend the regulations in the future, or could appeal. Planned Parenthood of Wisconsin v. Kaul, 384 F. Supp. 3d 982 (W.D. Wisc. 2019).

The legislature immediately appealed to the U.S. Court of Appeals for the Seventh Circuit. Because the Supreme Court's decision in Virginia House of Delegates v. Bethune-Hill had been decided after the district court's decision, the Wisconsin legislature had confirmed to the court that it was suing as an agent of the state itself, rather than as the legislature. The court of appeals affirmed the district court's application of the "bad faith or gross negligence" standard. Noting that the legislature "has the unenviable task of convincing a court that the Attorney General inadequately represents Wisconsin, despite his statutory duty," the court held,

If the Legislature were allowed to intervene as right, then it and the Attorney General could take inconsistent positions on any number of issues beyond the decision whether to move to dismiss, from briefing schedules, to discovery issues, to the ultimate merits of the case. The district court would, in that situation, have no basis for divining the true position of the State of Wisconsin on issues like the meaning of state law, or even for purposes of doctrines like judicial estoppel.
The court agreed with the legislature that the Wisconsin Attorney General’s authority is governed by state law and subject to the legislature’s control, and noted that the state could require the attorney general to withdraw and allow the legislature to take over. But, in this case, the legislature wants to litigate alongside the attorney general, which is “not an exercise of the State’s undoubted power to control the Attorney General, it is an attempt to control the proceedings in the court. We have no right to opine whether this law can have that effect on a state court, but even the Legislature concedes it cannot on a federal one.”

The court of appeals also voiced its concern about the effect of the legislature’s position on judicial administration. “Under the Legislature’s rule, a state could split its voice among as many entities as it wishes, and each would be able to intervene if it could meet the minimal standard that its interest may be inadequately represented. . . . Perhaps a state could even designate its individual legislators as agents and thereby flood a district court with a cacophony of voices all purporting to represent the state.”

Finally, the court of appeals affirmed the district court’s denial of permissive intervention for the legislature. Permissive intervention is discretionary in the trial court and is rarely overturned. The court of appeals held, “The court weighed the various parties’ interests and found that the value the Legislature added to the Attorney General’s representation of the State was outweighed by the practical complications that could have resulted from the State’s having two representatives at the same time.”


Endnotes
1  87 Ariz. 139, 141, 144 (Ariz.1960).
2  Howton v. Morrow, 106 S.W.2d 81, 82 (Ky. 1937).
3  Ky. SCR 3.0220.
4  Ky. SCR 3.022(b).
7  Id. at 1950.

About the Authors

Gina Cabrejo joined NAAG in January 2018 as its NAGTRI criminal justice instructor for Latin American programs. She was born and raised in Colombia, South America. She is a Colombian attorney who specialized in diverse areas of law, including finance, banking, criminal prosecution, and management. Gina has held national positions applying the rule of law and fighting corruption. She trained other Colombian prosecutors during the country’s transition to its oral accusatory legal system on “Principio de Oportunidad,” a type of negotiation settlement. As a governmental attorney working with the Office of the Attorney General in Colombia, Gina prosecuted complex corruption, tax evasion, financial crimes, and fraud cases. As a private attorney she counseled an investment bank in the merger of two companies. She possesses a master’s degree in International Law, LL.M. from Stetson University in Saint Petersburg, Florida, which complements her first degree in law. She is an exchange alumnus of the International Visitor Leadership Program. Given her expertise in inquisitorial and adversarial legal systems, she helps to facilitate trainings, increase communication and cooperation with other organizations, and develop domestic and international relationships for NAGTRI’s Center for International Partnerships and Strategic Collaboration (CIPS-C).

Emily Myers is NAAG antitrust and powers and duties chief counsel as well as NAGTRI chief editor. She has been with NAAG since 1993. She is the editor of NAAG’s recently published book, State Attorneys General Powers and Responsibilities (4th edition). Emily is also the author of chapters on state antitrust enforcement in American Bar Association and state bar publications. As antitrust counsel, she assists states in their multistate activities and maintains the NAAG Multistate Litigation Database, a comprehensive database of state antitrust cases since 1990.
When you write for the NAGTRI Journal, you share your legal knowledge and experience with over 11,000 subscribers, including AG office attorneys and district attorneys; you enhance your professional experience with a bylined article; and you join a distinguished group of authors contributing to the public service community.

Send us your idea(s) for an article you wish to write for a future issue of the NAGTRI Journal. Journal articles are sent to thousands of lawyers who are working in the public service domain. These are not law review articles. These are articles in which lawyers are writing for other lawyers. Sure, we like citations, but you will be writing on issues that you know well – that you handle every day in your job. No exhaustive research is necessary.

We know you can write. We know you have skills and knowledge in specialized fields. We also know that you find fulfillment in promoting the public good and in collaborating with colleagues. The Journal content leads readers to better serve the public in their various capacities. Help raise the profile of the excellent work that you and your AG office colleagues are doing by becoming a NAGTRI Journal author.

The Journal is issued quarterly. Articles have no word limit---say as much or as little as necessary to convey your idea, solution, or perspective. The time commitment is minimal compared to the outcome.

Interested? Email Emily Myers, emyers@naag.org with your article idea. Thank you!