WHITE PAPER

Law Enforcement Access to Evidence in the Cloud Era

THE CHERTOFF GROUP

Abstract: The transition to a global Internet economy has been accompanied by a significant change in the nature of law enforcement activity. Evidence that formerly was available within the boundaries of a single jurisdiction and could be collected through the operation of domestic law now is often collected, stored, and processed globally by transnational companies. As a result significant potential exists for the disruption of law enforcement activities because those who hold relevant evidence may be subject to conflicting legal obligations, unilateral actions by a single jurisdiction, and significant economic pressures. This white paper outlines the scope of the problem, surveys existing technical, legal, and policy conflicts and identifies potential responses to the changing dynamic.

I. Introduction

Historically, criminal investigations and prosecutions have involved matters of limited geographic scope. Evidence of a crime was most commonly physical evidence, not electronic, and it was typically to be found within the same jurisdiction as the locus of the crime itself. Less frequently, the evidence might be available in a neighboring state or local jurisdiction. Only in rare instances would the need exist to secure evidence from overseas using the Mutual Legal Assistance Treaty (MLAT) process.[1] That process was cumbersome, but in light of the nature of the relationship between evidence and the locus of a crime, that burdensome methodology had minimal practical impact on the vast majority of cases.

This is no longer the case. Today, some of the most relevant evidence of a crime is likely to be stored in an electronic format. And, given cloud structures and the global nature of the cyber-network, communications between two people in one country can be stored on servers half-way around the world. This burdens an MLAT system that is now asked to process requests for evidence that, prior to the development of the network, would never have been contemplated. Yet the MLAT process remains unchanged, essentially, from pre-Internet days and quite unwieldy. If law enforcement is to remain effective it needs to adapt to the reality that data and evidence is now global.

That same technological reality also has impacts on American (and foreign) technology companies. In some instances they may be faced with a dilemma, required to reconcile the obligation to respond to lawful requests from law enforcement yet also maintain competitiveness in foreign countries and comply with foreign legal obligations. In addition,

The MLAT process remains unchanged, essentially, from pre-Internet days and quite unwieldy. If law enforcement is to remain effective it needs to adapt to the reality that data and evidence is now global.

changing societal norms are driving the political domain to consider greater privacy protections for electronic files.

Many observers think that U.S. and global law enforcement have yet to develop a coherent approach to these new customs and practices. There has, thus far, been a failure to reach an accommodation on questions of reciprocity and to modernize the ability to swiftly secure electronic evidence. In the near term, this is creating problems for law enforcement and eroding the international standing of American corporations. In the long-term, given the globalized nature of the network, the status quo is unstable and cannot be maintained.

The time is ripe to revisit how electronic evidence relating to the content of communications and data is gathered by law enforcement for purposes of criminal prosecution in a particular country.[2] In an ideal world reform would both improve law enforcement access and regularize it while affording greater privacy protections to U.S. citizens and foreigners. This white paper outlines the scope of the problem, surveys existing technical, legal, and policy conflicts, and identifies potential responses to the changing dynamic.

II. Outline of the Problem

The new challenges to law enforcement evidence collection capability stem, fundamentally, from the changing nature of evidence – how it is created; how it is stored; and how it is accessed. That change arises from both technical aspects of how electronic data is stored and practical aspects of competing global legal systems. This section outlines these issues as a way of setting the baseline for further examination.

a. Technical

The Internet is a globe-spanning domain. As of late 2014, more than three billion citizens of the world were connected to the network.[3] Estimates vary, but somewhere on the order of 13 billion different devices are also connected – and those numbers will only grow exponentially in the coming years.[4]

The result is an increasingly common phenomenon – disputes and transactions that cross national boundaries. To be sure, the phenomenon is not new. There have been transnational commercial transactions and transnational criminal activity since the time that borders between nations were first created. But the growth of a system of near-instantaneous global communication and interaction has democratized the phenomenon of cross-border commerce in a transformative way that challenges and disrupts settled conventions.

The principal manifestation of the technological factor disrupting settled practices is the transition from on-premises computing to off-premise, shared computing services. These off-premise services, which may include data storage, processing, or application development, are colloquially referred to as "cloud computing." According to the National Institute for Standards and Technology, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[5]

Cloud computing is not a type of technology. Rather it is a concept of operations, comprised of multiple service and deployment models united by the idea of delivering computing as a service. Cloud providers maintain applications, data, and systems replicated on servers that are dispersed across any number of locations, connected to end users who access cloud services via web browsers, mobile applications, and other user interfaces.

Cloud computing is not a type of technology. Rather it is a concept of operations, comprised of multiple service and deployment models united by the idea of delivering computing as a service.

This cloud model is generally thought of as having five essential characteristics:

- On-demand self-service. Once a cloud system is set up, it operates independent, generally, of the service provider. A consumer can unilaterally add additional computing capabilities, such as server time and network storage, as needed, automatically without requiring intervening approval from each service provider.
- Broad network access. Cloud services can be accessed from anywhere on the network. So long as the consumer uses a standard mechanism on their platforms (e.g., mobile phones, tablets, laptops, and workstations) the data or services are universally available.
- Resource pooling. The cloud service provider's computing resources are pooled – in other words a provider's system of servers works for many clients at the same time and the provider reallocates its physical and virtual resources according to consumer demand. And that means, critically, that the service provided is not dependent on location – the resources may be provided from the cloud provider's most cost-effective location and the customer generally has no control over or knowledge of the exact location of the provided resources. The customer may, however, sometimes be able to specify a particular location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
- Rapid elasticity. The client can add or subtract services easily and quickly, in some cases automatically. This allows users to rapidly expand or contract their systems on demand. Given the nature of the cloud, its capabilities often appear to the consumer to be unlimited in quantity and available at any time.

- Measured service. Cloud services can be apportioned and measured readily. They may be "metered," for example, in terms of the storage, processing, bandwidth, and number of active user accounts. Because resource usage can be monitored, controlled, and reported, the service provider has insight into how the services it provides are used and the consumer has transparency as to the costs of service provided.

What this means, simply, is a transformation in how individual citizens use computing resources. Consider the simple example of stored electronic data. The user of a cloud-based data storage system (i.e. Dropbox™ or Spider Oak™) can use that storage capacity on demand, from anywhere in the world, as they wish, without the intervention of the service provider. They need no authorization, beyond the general one given when they purchased the service, to store a new document. Likewise, once stored in the system, they can access that data from any device they have – their laptop, their mobile phone or their tablet. If they need more storage space they can purchase it instantly, and their provider makes its profit by measuring their storage use and charging them accordingly.

Given the nature of the system, however, the user often (though not always) doesn't know where their data is being stored.[6] Typically, the service provider will make that determination based on cost- and efficiency-related factors. The data storage may take place close to the user (to speed service); where there is excess capacity; or where the costs of service (in terms of electricity, cooling, and manpower) are the least. Data centers may also be located in particular locations to take advantage of local law – as, for example, when a company gets a tax break to build a center in a particular city or country. Indeed, the final decision on storage will combine all of these factors and may well change on a very short time scale – that is, daily. As noted earlier, however, in a public cloud system,[7] the citizen/user will frequently have little or no control of where that is – it will be determined by the service provider.

Given the nature of the system, however, the user often (though not always) doesn't know where their data is being stored.

And that, in turn, makes clear the technical disruption that is effecting the ability of law enforcement to secure criminal content-containing evidence from the cloud. Typically, the evidence in question is data stored by, or records of usage of, a cloud customer. Those records and content are in the possession of a third-party, the service provider, but they may be stored anywhere in the provider's global system and relate to suspects or victims who are, likewise, beyond the jurisdictional bounds of law enforcement.

b. Legal

How, then, is an American law enforcement agency to proceed? What processes may be used to secure content evidence from a foreign company, with an American subsidiary, relating to a foreign criminal suspect who has allegedly victimized an American citizen, where the data is stored in yet another foreign jurisdiction?

The legal quandary is most noticeable when we consider the intersection between private commercial activities, criminal activity, and sovereign nations. Nations, quite naturally, seek to affect behavior through laws and regulations that apply to individuals and corporations within their jurisdiction. But the growth in cross-border commerce and criminality is rendering traditional choice-of-law rules problematic, at best. If one adds in the distributed structure of the network, inherent in the growing use of cloud architecture, the application of diverse legal systems to a unitary network becomes especially difficult.

What we see today, in response to this conundrum, is a three-fold problem:

- First, there are situations in which data holders are subject to conflicting legal obligations. Companies may be faced with mandated disclosure or delivery requirements that contravene other law. In Europe, for example, privacy laws may direct a company to refuse to respond to a US government investigative demand. Or, conversely, American privacy law might prevent a company from responding, say, to a Chinese or Russian investigative demand.
- This prospect leads directly to the second aspect of the problem – unilateralism -- that is the assertion by a nation that its laws control actions by evidence holders, irrespective of other countervailing interests. Increasingly, nations are putting mandates on citizens and/or service providers that are intended to effectuate their investigative interests. China, for example, has mandated that citizens register for access to the network and that providers maintain encryption back doors in products to enable access as a condition of being permitted to sell into Chinese markets. In addition, most jurisdictions preferentially protect the legal

rights and privacy of their own citizens over those who are not citizens of the sovereign. To the extent laws reflect these self-interested domestic principles unilateral action will, at some juncture, conflict with other legal obligations. To date, for the most part that has yet to occur, but it can be readily anticipated.[8]

As a result, localization rules are not self-executing and may increase confrontation at the cost of cooperation and will ultimately have harmful effects on innovation and economic development.

- The most prevalent form of such unilateralism is the increasing trend for sovereign nations to establish jurisdiction and control over matters they think are within their sphere of influence through legal mandates. These efforts fit under the general rubric of data localization requirements – the legal requirement that data about Germans, say, must be stored in Germany and subject only to German law. Even worse, such efforts may prove ineffectual: Though a nation like Germany can demand localization, other nations are not obliged to honor that determination and many nations' laws (for example, the UK's Data Retention and Investigatory Powers Act) apply extraterritorially. As a result, localization rules are not self-executing and may increase confrontation at the cost of cooperation and will ultimately have harmful effects on innovation and economic development.[9]

The future prospects for law enforcement in light of this situation is a time of uncertainty. For now, US law enforcement is still able to take advantage of American unilateralism, grounded in the circumstance that American companies dominate the market and that they can be compelled to assist American investigations. But this form of mandated assistance cannot be sustained in the long run. Even if the legal power to compel American companies to cooperate is sustained, they cannot provide that which they do not possess. A predictable reaction to such a legal régime is that American companies will lose market share because of these demands. They will be increasingly faced with stringent countervailing foreign law demands. Some nations may adopt both domestic storage requirements and, ultimately, domestic corporate preference requirements, both of which will increasingly put data beyond the effective reach of American criminal investigators.

Some nations may adopt both domestic storage requirements and, ultimately, domestic corporate preference requirements, both of which will increasingly put data beyond the effective reach of American criminal investigators.

More to the point, a continued American approach that asserts the primacy of American law will necessarily beget an equivalent response from foreign countries, to the detriment of American citizens and their privacy. When, for example, Alibaba opens its anticipated data center in Silicon Valley, American data stored in that center would be subject to Chinese unilateral demands – a result that derogates American privacy interests.

III. Effects

As we consider the current state of affairs, it is relatively easy to demonstrate that the status quo is having demonstrable effects on law enforcement practice, on the business model of global companies and, derivatively, on American privacy and civil liberties expectations. Some of those effects are positive, but the balance seems to tilt against the long-term viability of the current system.

a. Law Enforcement

Hard evidence of the costs to law enforcement that are derived from the current evidentiary access rules are difficult to find. Nonetheless we can readily see some indications that the current unilateralist practice of American law enforcement is beginning to have direct adverse effects on American investigations.

Nor is this problem unique to US law enforcement. Indeed, given the continued predominance of American service providers in the market, foreign nations are particularly challenged by the new cyber reality.

In the first place, evidence is becoming harder to identify and collect. Locations are being obscured and data is increasingly being placed beyond the reach of American law. For example, as a near-direct consequence of the Snowden revelations, Chinese customers are increasingly placing their data with Chinese cloud service providers – which, since the US has no treaty with China to secure access to that data, renders it virtually inaccessible.[10] Likewise, some nations with whom we do have treaties, such as Germany and Brazil, are considering data-localization requirements that would oblige U.S. law enforcement to proceed through the MLAT process by obliging data holders to place data to which the U.S. now has unilateral access beyond its jurisdictional reach.[11]

Nor is this problem unique to US law enforcement. Indeed, given the continued predominance of American service providers in the market, foreign nations are particularly challenged by the new cyber reality. If two French users in Paris communicate using an American service, French investigators can only access the content of that email conversation through the cumbersome MLAT process – delaying their investigation and requiring the expenditure of scarce American and French resources. Much as we value American primacy it is doubtful that interposing American courts into an entirely internal French investigation is either justified or justifiable.

Similarly, data holders themselves are increasingly interposing objections to the disclosure of evidence – if only as a way of attempting to reclaim the trust of their clients. Even when those objections are overcome, the costs of delay are quite real. More to the point, prospectively, the current law enforcement posture has led many American tech companies to openly oppose increased access by law enforcement to digital evidence.[12]

Meanwhile, in what is perhaps an even greater problem, the balkanization of evidentiary availability has created a number of safe havens for cyber criminality. According to Europol,[13] for example, the majority of attackers behind credit card data theft are from Eastern Europe, particularly Russian speaking countries that do no prioritize enforcement, and often lie beyond the reach of Western criminal jurisdiction.

To be sure, the trend toward greater use of cloud infrastructure has a number of significant benefits for law enforcement, not the least of which is that digital evidence usually provides a more definitive record of criminal acts. In addition, data in the cloud has significant forensic value beyond the data itself that is of utility to law enforcement investigations.[14]

And, as well, the U.S. today has a “home field advantage” in the cyber domain. Many of the largest tech companies are based in the United States and a significant fraction of network traffic still passes through American-based servers. Both those circumstances foster American law enforcement evidentiary access through unilateral demands.

But that home field advantage is fading. Estimates vary but it is clear that in the wake of the Snowden revelations, customers are increasingly turning to non-U.S. based companies to provide cloud services.[15] Indeed, expanding foreign cloud offerings has become a political and economic strategy of some of our largest trading partners[16] – a trend that will, in the end, significantly impact American law enforcement evidentiary access.

b. Transnational Companies

In some ways the costs of the current evidence-access legal structure to transnational corporations are the converse of the benefits to law enforcement. They range from compliance costs to burdens on their reputation and distortions of their business models.

The most obvious cost of the current system is the sheer complexity of it and the costs of compliance.[17] New European and Brazilian proposals, for example, are in potential conflict with American laws.[18] Inconsistent legal obligations put data holders in a nearly untenable position. Indeed, a patchwork of incommensurate laws makes it difficult, though not quite impossible, in some instances, to operate a conforming cloud-based data system.[19] According to the Business Software Alliance, legal and regulatory problems, including lack of legal protections and conflicts of law, have substantially impeded cloud computing growth.[20] That's why continued unilateralism and the growth of data localization are forecast to cause noticeable GDP, investment, and welfare losses.[21]

The most obvious cost of the current system is the sheer complexity of it and the costs of compliance.

The compliance costs are, however, just the tip of the iceberg for transnational tech companies. The current rules for law enforcement access to cloud-based evidence are effecting the perception of consumers and thus causing injury to their brands. Consumers outside the United States are losing trust in American tech companies.[22] Anecdotal evidence abounds that American companies are losing business because of perceived vulnerability to U.S. law enforcement evidentiary requirements.[23] Estimates vary as to exactly how much this will hurt the bottom line – some suggest that as much as $20-35 billion in revenue will be lost.[24] Other, more extreme estimates, suggest that impacts could be as high as $180 billion, which is 25% of the overall IT service provider's revenue.[25] Both estimates seem rather inflated – but the true costs are difficult to know with any certainty.

And then there is the official foreign government reaction which has, almost uniformly, been adverse to corporate interests (and, therefore, derivatively, adverse to American economic and security interests). The Irish government and the European Commission have both expressed a degree of dismay when it comes to how the U.S. Government seeks to obtain personal data stored outside their jurisdiction.[26] Brazil continues to work toward domestication laws that will change the business environment in that country.[27]

"In defense of Google and Facebook, sometimes the European response here is more commercially driven than anything else. As I've said, there are some countries like Germany, given its history with the Stasi, that are very sensitive to these issues. But sometimes their vendors — their service providers who, you know, can't compete with ours — are essentially trying to set up some roadblocks for our companies to operate effectively there."

- President Obama

Meanwhile, the Canadian government has suggested that it will offer incentives to American companies to move their data centers to Canada, outside American jurisdiction; the French and German governments have announced a joint initiative to create an EU-centric cloud, where data will be subject to EU privacy laws; and Brazil has announced an initiative with the EU to build a fiber-optic cable linking the two areas, allowing data to avoid transiting in the U.S.[28] More broadly, American relations with Germany have been greatly eroded,[29] with, perhaps, significant geopolitical effects beyond those experienced by American companies.

To be sure, some of this reaction has a commercial nationalism to it. As President Obama recently put it (to the chagrin of some European politicians): "In defense of Google and Facebook, sometimes the European response here is more commercially driven than anything else. As I've said, there are some countries like Germany, given its history with the Stasi, that are very sensitive to these issues. But sometimes their vendors — their service providers who, you know, can't compete with ours — are essentially trying to set up some roadblocks for our companies to operate effectively there."[30]

Nevertheless, whether commercially driven or derived from security concerns, the degradation in trust is real. Indeed it is so great that many speak of the need to restore what has been lost. More to the point, the EU is demanding changes in American law to protect EU users from U.S. intelligence and law enforcement.[31] Meanwhile, even the cornerstone of U.S.-EU data cooperation (the commercial Safe Harbor Agreement) may be reconsidered. That agreement allows for the

use of commercial data across the Atlantic despite differing privacy rules. Yet today, European authorities are questioning the continued vitality of Safe Harbor in light of US companies cooperating with US law enforcement and intelligence agencies.[32]

In short, despite the manifest benefits from a global network in terms of economic efficiency and better customer service,[33] the business model of transnational tech companies is at risk – not because of any change in the fundamental economics of the matter but simply because public and private perceptions have been so changed by recent events that the companies are losing the branding battle. And, as we've noted, if they lose the battle, law enforcement will lose the evidentiary access war.

As we go forward, and attempt to apply existing constructs to digital data we need to ask ourselves what the rules should be, rather than what they currently are since the latter is more a matter of historical accident than careful analysis.

This situation is not unique to digital data. There have always been limits to the government's powers to compel third-parties to provide it with evidence. Some are statutory (as with bank secrecy rules) and others are Constitutional in nature, but they assuredly exist. The government cannot, for example, order Verizon to wiretap its customers overseas. Nor can it subpoena Marriott for papers stored in a guest's hotel room. As we go forward, and attempt to apply existing constructs to digital data we need to ask ourselves what the rules should be, rather than what they currently are since the latter is more a matter of historical accident than careful analysis. In the end, the proper answer is a set of rules that balance all of the competing interests, including the security threats of today and the privacy interests of citizens.

IV. Potential Solutions

The current situation is untenable. Data localization and sovereign unilateralism will come with significant costs – both economic ones and social ones. Global companies will be subject to competing and inconsistent legal demands, with the inevitable result that consumers will suffer diminished access to the network overall. Among other things, decisions about the location of servers and hardware will be driven by legal gamesmanship rather than technological or infrastructure considerations.

What would such a framework look like? It would, reasonably, have two parallel components. The first is a set of choice of law rules, so that evidentiary disputes would be resolved according to a pre-existing set of rules.

Meanwhile, law enforcement will increasingly find their legitimate investigative needs frustrated. Disruptive localization rules will move data that was formerly available outside of their jurisdictional reach. Disputes over jurisdiction will delay responses. And even when jurisdiction is definitively determined, delays will ensue as the cumbersome MLAT process is invoked. Left unaddressed these problems will only worsen.

To begin with, every Nation defines its own jurisdictional rules. As a result, we have to consider how these rules will be applied to American interests reciprocally. For example, under United Kingdom law, the presence of a subsidiary in that country binds the parent corporation to British data access rules. To cite another example, Brazil's law precludes the disclosure of Brazilian customers' data to any other government. Likewise the Electronic Communications Privacy Act (ECPA) has a prohibition on disclosure by American companies. Yet, both countries purport to require data holders to turn the data over to them no matter where it is stored. So, both countries essentially tell service providers that they must follow the law and that their laws have primacy – even when the laws conflict.

This patchwork of jurisdiction will ultimately undermine investigations and will only get worse as more and more countries follow their lead. The current free-for-all of competing nations needs to be replaced with an agreed upon international system that would harmonize and improve upon existing rules and processes within an agreed upon framework of law.

What would such a framework look like? It would, reasonably, have two parallel components. The first is a set of choice of law rules, so that evidentiary disputes would be resolved according to a pre-existing set of rules. The second, would be a significant improvement in the MLAT process so that recourse to foreign governments for assistance would not be delayed by bureaucratic lethargy.[34]

a. Choice of Law[35]

In contemporary cloud structures, data is often stored in more than one location, either in disaggregated form or with copies resident in more than one data center.

The principal question that will need resolution is the simple one of "whose law applies?" If we are to replace a unilateral response of "mine; no mine" with an agreed framework, the United States will need to advance a neutral choice of law system that is agreed upon on a bilateral or multilateral basis. This choice of law framework could take many forms:

One approach would carry the data localization movement to its logical conclusion and hold that the law of the country where the data resides controls access to it and rules relating to its processing. This parallels the usual case with physical evidence. Under such a system, for example, a case involving data held, say, in Ireland would be resolved by applying European and/or Irish law. This choice-of-law rule would have the virtue, at least, of clarity. Everyone concerned would know which jurisdictions' law would control.

But in many ways this clarity is illusory. In contemporary cloud structures, data is often stored in more than one location, either in disaggregated form or with copies resident in more than one data center. It may also transit through multiple physical locations. A data localization choice-of-law rule would force corporations to alter the most economical structures of their data systems in order to secure legal certainty – an unnecessary cost. Alternatively, the data holders might choose not to take these costly steps, thereby creating the very legal uncertainty the rule is intended to avoid.

Perhaps more importantly, a data localization choice-of-law rule would create perverse incentives. Technologically, the most economically efficient place to store data is a product of a number of factors such as climate, infrastructure, and proximity to users. With a localization choice-of-law rule we can anticipate at least

two inefficient responses: First, some jurisdictions, either out of legitimate concern for their citizens or an authoritarian interest in control, will see this legal rule as a license to mandate inefficient local storage requirements. Second, conversely, we might see other jurisdictions in a "race to the bottom" as they attempt to create data access rules that are favorable to the data holders as a way of attracting business interests. Still others might develop rules that make them data access "black holes" where malicious actors can find a safe haven from legitimate law enforcement scrutiny. None of these results is optimal – leading one to question such a formulation of the choice-of-law rules.

Instead one might consider a different formulation (or, rather, four alternate formulations) that will also provide clarity in defining the jurisdiction that controls while being systematically less susceptible to economic gamesmanship and rent-seeking than a data location rule. One might consider either a choice-of-law rule based on the citizenship of the data owner OR the citizenship of the data subject OR one based on the location where the harm being investigated has taken place OR one based on the citizenship of the data holder or custodian.

To be sure even these rules will, at the margins, have grey areas. Some data subjects may be dual citizens. Some data holders may have corporate headquarters in more than one nation. And some events may give rise to harm in more than one location. But none of these are circumstances that are as readily capable of manipulation as data location – indeed in many instances they will be extrinsic to the data and the product of other circumstances.

There are sound arguments for and against each of these possible rules:

- A rule based on citizenship would ground internet jurisdiction in a familiar legal construct. It would also reinforce the idea that citizenship and sovereignty are closely linked. It might, however, be the most difficult rule to implement technologically, since data often does not have a flag for citizenship of origin or ownership and adding such a marker might prove challenging, if not impossible, retrospectively.
- A rule based on corporate citizenship would have the virtue of ease of application – a single rule would apply to all data held by the data holder. It would also, however, have the unfortunate effect of creating transnational incentives of the same sort as a data localization rule, with the added consequence of fostering economic nationalism.
- A rule based on the location of harm seems the least capable, generally, of manipulation and most directly linked to cognizable sovereign interests. It suffers, however, from the ability of sovereigns to define and manipulate the definition of harm and would only be implementable for certain universally agreed upon harmful acts, such as, for example, murder.

To be sure, none of these rules is perfect. Each is capable of manipulation and each will require some transnational cooperation to implement. The virtue, however, of these suggested rules lies in their ability to create clarity and ease of use among willing participants. One could, for example, imagine a transnational agreement on data availability tied to the protection of life and property, perhaps with some degree of judicial oversight, which could be implemented throughout the West. That limited goal, by itself, would be a major achievement in creating security, clarity, and consistency on the network while, in the long run, fostering law enforcement evidentiary access.

b. MLAT reform

Revised choice of law rules will give certainty to jurisdiction, but they will not address the full scope of the problem unless accompanied by a means of promptly and effectively securing the exercise of that jurisdiction. When the matter involves an inquiry outside the jurisdiction of the nation seeking the data, requests for assistance under any choice-of-law rule will have to be processed through MLAT-like channels. These channels are considered cumbersome, at best.

> Revised choice of law rules will give certainty to jurisdiction, but they will not address the full scope of the problem unless accompanied by a means of promptly and effectively securing the exercise of that jurisdiction.

Hence an effective response to the problem of transnational evidentiary issues also requires a modernization of the MLAT process. Such a modernization is likely to encompass three important components – process improvements; reciprocity obligations; and an accommodation for circumstances that are exigent.

Process improvements will necessarily involve changes in the timeliness and security of the MLAT system. Complaints about MLAT implementation routinely call out the lack of a prompt and automated response.[36] The outlines of an improved system are readily apparent. They include: secure, automated connectivity between law enforcement agencies and a presumptive time limit for response. The time limit might conceivably be tied to the nature of the case, with a longer agreed-upon limit for routine matters, but the central point would be that signatories bind themselves to meeting performance objectives tied to the pace of a response. In the increasingly rapid age of cybercrime and cyber espionage more use of rapid response mechanisms is essential.

A second keystone of MLAT reform would be reciprocity. Nations would bind themselves to forego the exercise of unilateral evidentiary methods. But this sort of agreement would only be effective if both parties make reciprocal commitments as to the exclusivity of the MLAT mechanism and as to its responsiveness. In other words, the US could agree to use non-unilateral MLAT means of evidentiary exchange as to matters within the jurisdiction of another nation, but only if that nation reciprocally agreed to do likewise with respect to evidence within American jurisdiction and if it, similarly, bound itself to respond to MLAT requests from the US in a timely manner (a promise that the US would also make and which might well require the Federal government to improve its own responsiveness to foreign inquiries).

Finally, newly negotiated MLAT agreements should also consider the circumstances in which an exigency requires bypassing agreed upon processes and returning to more unilateral measures. One could imagine that such situations involving ongoing events where even the revamped MLAT processes would be too cumbersome. Plausibly, this exigency provision might be limited to serious transnational crimes involving imminent threats of death or serious bodily injury. It might also require some form of consultation before unilateral measures were exercised. But in the end, law enforcement interests may well require some residual form of unilateral self-help by law enforcement in extraordinary circumstances.

V. Conclusion

This white paper is not intended to endorse any particular solution to the conundrum of law enforcement evidentiary access in the cloud-era. It is, however, intended to make clear two things: a) that the status quo of competing unilateralism is costly and, in the long run untenable; and b) that responsible solutions can be crafted that are consistent with existing technical challenges and evolving societal norms but do not cripplingly encumber law enforcement activity. American law enforcement should embrace the challenge of finding a reformed mechanism for evidentiary access and welcome the opportunity to participate in the debate about its contours. The current tumult is, to be sure, a threat to settled expectations, but it is also an opportunity for modernization that should not be feared.

About The Chertoff Group

The Chertoff Group is a premier global advisory firm focused exclusively on the security and risk management sector. The Chertoff Group helps clients grow and secure their enterprise through business strategy, mergers and acquisitions and risk management services. The Chertoff Group, and its investment banking subsidiary Chertoff Capital, have advised on multiple M&A transactions totaling nearly $7 billion in deal value. Headquartered in Washington D.C., the firm maintains offices in Austin, Houston, London, Menlo Park and New York. For more information about The Chertoff Group, visit www.chertoffgroup.com.

Endnotes

1 An MLAT is a formal agreement between two or more nations regulating the exchange of information between them for public or criminal law purposes. Typically, the process requires a domestic prosecutor to convey a request for information to the Department of Justice which will transmit the request to the foreign nation where the request will be adjudicated under that nation's laws.

2 Separate laws govern the collection of "non-content" data which, historically, has been considered distinct from content. Likewise, both content and non-content data may be collected through surreptitious means of espionage. This white paper is focused exclusively on the exchange of content-containing electronic data across global boundaries in the pursuit of law enforcement activities

3 Internet World Stats, http://www.internetworldstats.com/stats.htm.

4 BBC, 500 Billion device will be connected to the Internet by 2030 (August 2014), http://www.bubblews.com/news/5630913-500-billion-device-will-be-connected-to-the-internet-by-2030.

5 Timothy Grance and Peter Mell, NIST Special Publication 800-145: "The NIST Definition of Cloud Computing," National Institute for Standards and Technology, September 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

6 Some providers publish information about their data center footprint, and some companies may insist upon control over data location and, therefore, know which data center or country/region their data resides in.

7 The cloud architecture may be deployed by a public company as a service to an undifferentiated group of consumers (known as a public cloud) or by a private company to its own employees or customers (a private cloud). In terms of structure there is little difference to the deployment model. In legal terms, as we shall see, the public cloud is far more challenging of settled law enforcement models of evidence collection.

8 BBC, US tech firms ask China to postpone 'intrusive' rules, (January 29, 2015), http://www.bbc.com/news/technology-31039227.

9 We discuss this issue more broadly in § III, *infra*. For a useful introduction to the economic and social costs of data localization proliferation, *see* Jonah Force Hill, The Growth of Data Localization Post-Snowden: Analysis and Recommendations for US Policy Makers and Industry Leaders, *Lawfare Res*. Paper Ser. Vol. 2, No. 3, (July 2014), http://www.lawfareblog.com/wp-content/uploads/2014/07/Lawfare-Research-Paper-Series-Vol2No3.pdf.

10 Tech 2: China tech firms benefit from US spying allegations, Snowden revelations (May 30, 2014), http://tech.firstpost.com/news-analysis/china-tech-firms-benefit-us-spying-allegations-snowden-revelations-224738.html.

11 FCW: Cloud computing under siege (September 12, 2014), http://fcw.com/Articles/2014/09/12/cloud-under-siege.aspx.

12 For example, the current proposal to change the geographic limits in Rule 41 of the Federal Rules of Criminal Procedure which might, at a different time, have been seen as a ministerial modernizing update are now the subject of vigorous criticism and opposition. *E.g.* Gigaom: Google raises alarm over global search warrants (February 18, 2015), https://gigaom.com/2015/02/18/google-raises-alarm-over-global-search-warrants/

13 EUROPOL: The Internet Organised Crime Threat Assessment (2014), https://www.europol.europa.eu/sites/.../europol_iocta_web.pdf.

14 Crosstalk: Digital Forensics in the Cloud (August/September 2014), http://www.crosstalkonline.org/storage/issue-archives/2013/201309/201309-Zawoad.pdf.

15 *E.g.* ITIF, How much will PRISM cost the US Cloud Computing Industry, www2.itif.org/2013-cloud-computing-costs.pdf; Financial Times: Cloud computing industry could lose up to $35Bon NSA Disclosures (August 5, 2013), http://www.ft.com/cms/s/0/9f02b396-fdf0-11e2-a5b1-00144feabdc0.html; CNBC: Foreign cloud companies will win big from NSA spying revelations (March 31, 2014), http://www.cnbc.com/id/101540029.

16 EU: European Cloud Computing Strategy (September 2012), http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy.

17 Ecommerce Times: Will Data Localization Kill the Internet? (February 10, 2014), http://www.ecommercetimes.com/story/79946.html.

18 Forbes: How Brazil and the EU are breaking the Internet (May 9, 2014), http://www.forbes.com/sites/elisugarman/2014/05/19/how-brazil-and-the-eu-are-breaking-the-internet/.

19 Business Computing World: Global Patchwork of Conflicting Laws and Regulations Threatens Cloud Computing (February 23, 2012), http://www.businesscomputingworld.co.uk/global-patchwork-of-conflicting-laws-and-regulations-threatens-cloud-computing/.

20 Business Software Alliance: 2013 BSA Global Cloud Computing Scorecard (March 2013), http://cloudscorecard.bsa.org/2013/assets/PDFs/BSA_GlobalCloudScorecard2013.pdf.

21 European Centre for International Political Economy: The costs of data localization (April 22, 2014), http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf; *see also* Hill, Data Localization, *supra* n.9.

22 CNET: US spying scandal will 'break the Internet,' says Google's Schmidt (October 4, 2014), http://www.cnet.com/news/us-spying-scandal-will-break-the-internet-says-googles-schmidt/.

23 *E.g. The Hill: Tech companies fret over loss of consumers' trust after NSA revelations (June 24, 2013), http://thehill.com/policy/technology/307183-tech-companies-fret-over-loss-of-consumers-trust; Business Insider: The NSA Leaks Are Starting To Hit The Bottom Lines Of Tech Companies (August 27, 2013), http://www.businessinsider.com/prism-the-nsa-leaks-are-starting-to-hit-the-bottom-lines-of-tech-companies-2013-8; The Hill: Why US cloud companies and the economy are under threat (October 14, 2014), http://thehill.com/blogs/congress-blog/technology/220332-why-us-cloud-companies-and-the-economy-are-under-threat.*

24 *See* ITIF, How much will PRISM cost the U.S. Cloud Computing Industry, www2.itif.org/2013-cloud-computing-costs.pdf; *see also* Financial Times: Cloud computing industry could lose up to $35Bon NSA Disclosures (August 5, 2013), http://www.ft.com/cms/s/0/9f02b396-fdf0-11e2-a5b1-00144feabdc0.html; CNBC: Foreign cloud companies will win big from NSA spying revelations (March 31, 2014), http://www.cnbc.com/id/101540029.

25 Forrester: The Cost of PRISM Will Be Larger Than ITIF Projects (August 14, 2013), http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects.

26 RTE: Irish Government seeks EU support in Microsoft data case (November 18, 2014), http://www.rte.ie/news/2014/1118/660564-tech-data-commission/; ZDNet: Microsoft ordered to hand over overseas email, throwing EU privacy rights in the fire (July 31, 2014), http://www.zdnet.com/article/microsoft-ordered-to-hand-over-overseas-email-throwing-eu-privacy-rights-in-the-fire/.

27 Reuters: Brazil to insist on local Internet data storage after US spying (October 18, 2013), http://www.reuters.com/article/2013/10/28/net-us-brazil-internet-idUSBRE99R10Q20131028; Wall Street Journal: Brazil Legislators Bear Down on Internet Bill (November 13, 2013), http://www.wsj.com/articles/SB10001424052702304868404579194290325348688.

28 Paul Rosenzweig, What is the cost of a Snowden?, Safegov.org (March 26, 2014), http://safegov.org/2014/3/26/what-is-the-cost-of-a-snowden.

29 The Guardian: Germany seeks EU support for online privacy charter after NSA revelations (July 24, 2013), http://www.theguardian.com/world/2013/jul/24/germany-eu-charter-online-privacy-nsa.

30 Obama: The Re/Code Interview (February 15, 2015), http://recode.net/2015/02/15/white-house-red-chair-obama-meets-swisher/.

31 EU: Restoring Trust in EU-US data flows- Frequently Asked Questions (November 27, 2013), http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm.

32 Practical Law: The Future of the US-EU Safe Harbor (December 2013), https://www.huntonprivacyblog.com/files/2013/12/Privacy-Data-Security-The-Future-of-the-US-EU-Safe-Harbor.pdf.

33 The economic efficiency of the cloud is well-known, as is its value to consumers. Useful summaries include: Forbes: The Economic Benefit of Cloud Computing (September 17, 2011), http://www.forbes.com/sites/kevinjackson/2011/09/17/the-economic-benefit-of-cloud-computing/; CIO Magazine: How cloud Computing Helps Cut Costs, Boost Profits (March 12, 2013), http://www.cio.com/article/2387672/service-oriented-architecture/how-cloud-computing-helps-cut-costs--boost-profits.html; Forbes: Making Cloud Computing Pay (April 10, 2013), http://www.forbes.com/sites/louiscolumbus/2013/04/10/making-cloud-computing-pay-2/.

34 We note that Congress has begun consideration of this issue – at least of the later portion concerning MLAT reform. With the LEADS Act, S. 512 the Senate has taken initial steps to address international concerns and improve the process. Some Congressional action is a necessary first, but not sufficient step in reform.

35 This section, in particular, is directly derived from the Global Commission on Internet Governance publication "A Primer on Globally Harmonizing Internet Jurisdiction and Regulations" by Michael Chertoff and Paul Rosenzweig. https://ourinternet-files.s3.amazonaws.com/publications/gcig_paper_no10_0.pdf

36 Global Network Initiative: Data Beyond Borders- Mutual Legal Assistance in the Digital Age (January 2015), http://csis.org/files/attachments/GNI%20MLAT%20Report.pdf.