Statement for the Record
by
The Honorable Michael Chertoff
Co-Founder & Executive Chairman of
The Chertoff Group
and
Former Secretary of the
U.S. Department of Homeland Security

U.S. House Judiciary Committee Hearing:
"International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests"

Thursday, February 25, 2016

STATEMENT FOR THE RECORD
BY THE HONORABLE MICHAEL CHERTOFF
UNITED STATES HOUSE JUDICIARY COMMITTEE
FEBRUARY 25, 2016

I want to thank Chairman Goodlatte, Representative Conyers and members of the Committee for inviting me to testify and for the opportunity to contribute to this important discussion. I am hopeful that discussions like these today will ultimately contribute to a better understanding of how our world has changed when it comes to the way we use data and where possible reforms may be necessary to update laws and policies that reflect today's environment.

I want to state clearly that I am testifying today and submitting my Statement for the Record in my personal capacity, although, for the record, I am co-founder and executive chairman of The Chertoff Group, a security and risk management company that provides strategic advisory services on a wide range of issues, including those we may discuss today. As I communicated previously to the Committee, The Chertoff Group does have technology clients interested in the topic of this hearing, including Microsoft who is also testifying as a witness today. However, I am not representing any specific company at this hearing and I will provide my opinion and testimony based on my own experience and understanding of the issues. Additionally, I also serve as Senior of Counsel to the law firm of Covington and Burling, LLP, which is counsel to Microsoft in a related litigation, although I am not personally engaged in that representation.

Today we live in a world shaped by a global digital economy – an economy made possible by the networking and communications infrastructure of the Internet which has enabled individuals, businesses and institutions, and governments to communicate, collaborate, trade and conduct business in a way never imagined before. The singular characteristic that defines our global cyber network is its universality. It is the Internet's ability to make information available instantly on a global scale which has enabled critical communications and services essential to our way of life.

The Internet was started more than 30 years ago by a small group at Stanford University in response to a government request to create a small, collaborative environment to be used by a

small group of trusted users. Security was never a concern because the group of users was small and known to each other. It was designed to be free, open, flexible and efficient.

Today, the Internet is a globe-spanning domain. More than three billion citizens and six billion devices are connected to the Internet. Its value proposition is that it is an open network of networks. As we work to preserve the openness of the Internet, we must do so through collaboration between the private sector, government, and the broader international community.

Today, I want to address some of the unique challenges we face in this global Internet economy and how, we … speaking collectively across government and industry … can best govern and secure the Internet in a way that protects public safety and enhances privacy without creating barriers that will diminish the important benefits we yield today.

The transition to a global Internet economy has been accompanied by a significant change in the nature of how we communicate, conduct transactions and exchange commerce. Today, we see a world through data. Our smart phones and devices hold vast amounts of data relating to our personal lives as well as daily business interactions. This data is not stored in any one specific place but today, it is often stored in the "cloud." To be clear, data stored in the cloud still resides on a physical server; however, the location of the server and where the data is ultimately stored can be anywhere around the world and is often determined based on several factors such as the location of the customer; facility resources (for example, adequate power and cooling capacity); and cost effective business environment. As a result, servers in one country can be storing communications between two people in another country.

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.

These challenges and disruptions have led to uncertainty including:

- Conflicts with regard to whose laws govern data held in cyberspace;
- Unilateralism or assertion by nations that its laws control actions by evidence holders, irrespective of other countervailing interests; and
- Global companies subject to competing and inconsistent legal demands where one country may require disclosure of information that another country prohibits from being disclosed

These issues pose challenging questions from a legal standpoint about who has jurisdiction over data held elsewhere and how one governs data in the cloud? How do we modernize our laws in a way that balances legitimate public safety needs and lawful access requests with the security and privacy of our citizens?

Without resolution or agreement on rule of law, all of this uncertainty contributes to concerns that these conflicts can lead to fragmentation of the Internet as we know it today. It could lead to second and third order effects such as data localization. If we don't figure out a new way of resolving legal conflicts, the universal Web as we know it may soon be Balkanized. We will lose the free and openness of the Internet as we do today and sacrifice the benefits that has brought incredible advances in our society.

The inevitable result will be that consumers suffer diminished access to the network overall. Decisions companies make about the location of their servers and hardware will be driven by legal gamesmanship rather than by technological or infrastructure considerations. We should work together to identify an agreed-upon international system for newly designed choice-of-law rules for data, particularly data in the Internet cloud. Such rules would determine which country's law governs in a dispute, as when we try to decide whose law governs a contract for the sale of goods. We need to harmonize existing rules in a framework of law for the cyber age.

For consideration, here are a few principles that ought to guide us going forward:

- Rules imposing localized requirements for data storage, processing, retention and distribution distort markets and create uncertainty. We should preferentially choose globalized rule-sets that apply across the entire domain, rather than nation-specific rules that add unnecessary costs and may even impose significant conflicting obligations;

- Because we need globally applicable rules, there will be challenges in securing world-wide agreement. Accordingly we need to work together and identify the smallest set of rules that are universally acceptable and necessary to the functioning of the network;

- In those instances where the laws of two countries conflict, we need an overarching choice of law agreement that determines which law controls based, preferably, on the citizenship of the individual account holder.

As previously mentioned, the overall public benefits resulting from new opportunities and innovation relating to the Internet have also brought forward new opportunities for criminal activity as well. Together, the way communication and information is exchanged has created new challenges for law enforcement. Fundamentally, it has changed the 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.

The Mutual Legal Assistance Treaty or MLAT process - the system by which law enforcement cooperate across borders – is hopelessly outdated. The President's Review Group on Intelligence and Communications Technology reports that the average length of time it takes for the U.S. to secure a response to its requests for evidence from foreign police partners is 10 months. And doubtless the converse is true as well – American responsiveness is also tedious and slow. None of this is adequate.

As our Congress considers reforms, we should highlight the need for reciprocity. American improvements will be insufficient if they are not matched by our partners around the globe. An

improved and functioning MLAT process would also have the collateral benefit of incentivizing nations to forego the exercise of unilateral evidentiary collection methods.

There is no doubt that issues concerning technology, data access, security and privacy within this globe-spanning Internet domain will continue to evolve as forecasts call for tremendous growth in the numbers of users and devices connected to the Internet. We do have an opportunity, however, to bring forward significant security reforms that can protect the greater public good without harming the digital economy which is also an essential element of our national security. Enhancing privacy and security, as well as providing clarity and consistency with regard to how we govern and apply rule of law, would be major achievements in this current environment.

###