Policy recommendations

Government access to data

The opportunity

Cloud technologies offer enormous potential, not only to spark innovation and efficiency but also to serve as a secure location for storing confidential and sensitive information. Businesses and individuals have the reasonable expectation that the information they create and store in digital form should be accorded the same privacy protections as information they commit to paper.

The challenge

To fight crime and protect public safety, governments have a clear and compelling need to access digital data. Balancing that interest against their citizens' expectation of due process and the rule of law is essential to maintaining trust in technology. This makes it a critical priority to craft modern laws that provide law enforcement and national security agencies with appropriate mechanisms to access digital information pursuant to lawful process. These laws should protect citizens' fundamental privacy rights, and respect the sovereignty of other nations.

In addition, the rapid adoption of cloud services coupled with the corresponding rise in transnational criminal activity raises new challenges for law enforcement. But because most countries' laws have not kept pace with technology, today when information is moved to the cloud, there is uncertainty about the legal frameworks that govern access to private information.

In addition, because of the lack of international frameworks for accessing digital evidence, governments are increasingly taking unilateral steps to seize information stored outside their border. This can create unresolvable jurisdictional conflicts that may undermine laws or force companies to have to choose to disregard the laws of one country in order to comply with the laws of another.

Rather than circumvent established mechanisms for cross-border cooperation, it is incumbent upon governments to modernize outdated systems and, where necessary, create complementary mechanisms that operate with the efficiency required to meet today's challenges and safeguard time-honored values, including privacy and human rights.

Policy recommendations

To enable law enforcement agencies to protect public safety, governments sometimes require access to digital information, including data stored in the cloud. However, in doing so, they can undermine public trust in cloud computing.

Therefore, it is important that governments strike a balance between public safety on one hand and personal privacy and freedoms on the other by adopting clear legal rules for seizing digital evidence. In developing such rules, governments should consider the following:

Allow access to digital information only pursuant to lawful process. Any framework regulating a government's ability to access digital information stored with technology providers must begin by recognizing the general principle that all access should be pursuant to the rule of law.

Right of technology providers to challenge. Technology providers should have the opportunity to challenge such process on behalf of their customers to ensure that governments are acting within the law and are respecting the rights of their users. This is a critical check on the use of government investigative powers—one that has proved effective in the United States.[13]

Require rigorous forms of legal process for more sensitive information. Technology companies store at least three types of information for their customers: (1) content, which includes information in emails and other electronic files; (2) noncontent information, which includes information relating to a user but excludes user content; and (3) subscriber information, such as identifying details about the subscriber of a service. Content is the most sensitive category of data because it contains the substance or meaning of a person's communications or documents. It is therefore appropriate to require more rigorous forms of legal process—subject to additional layers of judicial oversight—when the government seeks to access content. Though democratic governments around the world will determine their own appropriate standards, the U.S. requirement of a warrant for the seizure of content—issued by a neutral magistrate based on a finding of probable cause—offers a model that is worth considering.

Authorize disclosure in emergencies. Although governments should only be permitted to access digital information stored in the cloud through lawful process, narrow exceptions may be appropriate for emergency situations, such as when there is a reasonable, good faith basis to believe that access is needed to avoid death or serious physical injury. Such an exception can be especially crucial when law enforcement agencies face an ongoing emergency. Though the occasions when this type of exception are required are likely to remain relatively rare (as evidenced by Microsoft's annual transparency report, which includes the number of emergency requests it receives by country), such exceptions can save lives.

Support transparency. In recent years, the technology industry has secured the right to publish aggregate data about the number and types of requests it receives for digital evidence. In addition

to laws that permit this level of transparency, governments should allow companies to publish detailed information (including the number of requests received and the number of customers impacted) in order to ensure that the public can understand how governments exercise their investigative authority over information stored in the cloud. Technology companies have been publishing information about law enforcement requests for years, and in 2014, new levels of transparency on the part of the United States helped demonstrate that similar information about national security requests can be made available to the public.[14]

User notice. Except in limited cases, individuals and organizations have a right to know when governments access their digital information. Secrecy should be the exception not the rule. When secrecy is required, investigators should make their case to an independent authority, such as a judge. Governments should be required to provide case-specific facts to justify any limitations on the cloud provider's ability to notify its customers of the request. And, just as important, any nondisclosure obligations imposed on a cloud provider should be limited in duration and scope to the narrowly defined objectives of the specific investigation. When necessary, cloud providers should be permitted to challenge these orders to ensure that governments operate within the law. Though it remains inadequate and in need of significant improvement, U.S. law that governs the issuance of gag orders in criminal cases is better than analogous laws in many other countries.

Modernize rules governing appropriate targets of requests for cloud data. With more and more public and private organizations moving their digital information to the cloud and many newer companies using cloud-based infrastructure to deliver applications and services to customers, governments often have multiple sources for the digital information they seek.

Whenever possible, digital evidence should be obtained from the company most directly offering the service to customers—which in many cases will not be the cloud provider. In our view, this can often be done without jeopardizing an investigation. In situations where this approach would jeopardize an investigation, governments should be required to direct the legal process at the customer instead.

Respect international borders and sovereignty. The lack of modernized laws and international frameworks for accessing digital evidence and the increase in unilateral actions by law enforcement agencies to seize information stored outside their border threatens to erode consumer trust and is creating difficult legal situations for companies that provide cloud services. The existing mutual legal assistance process should be modernized and streamlined to ensure that it can continue to serve its purpose in a modern world. To do that, governments should develop a system that empowers law enforcement agencies to combat the many threats we face today, from terrorism to cybersecurity, while strengthening global protections for human rights and privacy, and promoting the free flow of information. Important work is already being done in this area by academics and a small number of governments seeking to develop a model that can be widely replicated.

Promote trust through security. In recent years, law enforcement agencies have argued that encryption impedes legitimate investigations by putting encrypted information beyond their reach. However, some of the proposed solutions to this issue—from weakening encryption algorithms to mandating that governments be provided with encryption keys—raise significant concerns. Encryption plays an important role in protecting private data from hackers and other malicious actors. Regulatory or legal reforms in this area must not undermine security, an essential element of users' trust in technology.

Evidence and further reading:

Reform of Government Surveillance Blog: RGS Statement on US-UK Data Protection Discussions

Microsoft Blog: Keeping secrecy the exception, not the rule: An issue for both consumers and businesses

Lawfare: "Cross-Border Data Requests: A Proposed Framework"

Just Security: "Privacy Rights Advocates Embrace DOJs Cross Border Data Proposal"

The Guardian: "Tech giants reach White House deal on NSA surveillance of customer data"

For links to these and other resources, please visit:
http://www.microsoft.com/cloudforgood