

November 2009

**Privacy and Data Access in a World
of Online Computing: A Call To Action**

Summary

A new generation of technologies is transforming the world of computing. The traditional model of computing—with software running on a user’s own PC or a business’s on-site computers—is increasingly being augmented by computing delivered as a service over the Internet. This computing model—often called “cloud” computing—offers tremendous opportunities, giving enterprises and consumers greater choice and flexibility while driving significant efficiency gains, lowering IT costs, and creating incentives and online platforms for innovation. These technologies, like earlier advances in IT, hold great promise for spurring economic development and job growth.

Long-term investment and innovation in cloud computing, however, are being threatened by a global legal quagmire. National governments are imposing conflicting legal obligations and asserting competing claims of jurisdiction over user content and data held by online computing service providers. Divergent rules on data privacy, data retention, law enforcement access to user data, censorship, national security, and other issues are placing providers in an impossible, Catch-22 position, with several companies facing protracted legal battles and substantial fines in foreign courts and threats of imprisonment for their employees. If companies are forced always to store data locally to mitigate these jurisdictional conflicts, the costs for investment and innovation in cloud computing will increase, many of the efficiency and performance gains of cloud computing may be lost, and the benefits to users will be reduced.

Consumers and governments also have important interests at stake. Consumers, much like businesses, have a fundamental interest in knowing that their online data is subject to consistent, predictable privacy protections. Consumer confidence in the security and privacy of online computing will not exist, however, without clear and consistent rules governing who may access the data and under what circumstances.

For their part, governments have interests in realizing the efficiencies and economic benefits that online computing offers, while also advancing the safety of the online environment and protecting government and private-sector networks and assets. Safeguarding these interests in the emerging online computing world presents significant challenges. In particular, governments must be able to support the development and use of online computing while protecting the privacy and security of their citizens’ data. At the same time, governments also must grapple with the dynamic threats that the online computing environment can present. The fact that these threats arise in an interconnected environment—one in which there is a simultaneous diffusion and instant connection of data, a greater ability for criminals to obscure their identities, and uncertainty over the application of traditional notions of jurisdiction—can greatly complicate governments’ ability to lawfully access data for legitimate law enforcement and national security purposes. These complications are amplified by a growing thicket of conflicting legal obligations, which make it more difficult for providers to respond quickly even to government demands that are clearly legitimate.

Industry has been working hard to address these problems, but cannot solve them alone. It is essential that governments around the world step in to help craft new guidelines and processes to ensure the privacy and security of user data, and to provide consistent rules and clear guidance on lawful government access to user data. Globally consistent rules are vital to achieving these goals and to realizing the many benefits of the next generation of computing.

I. The Shift to Online Computing and Its Benefits

Over the past several years, the Internet has radically redefined the way we communicate, access content, and share information. Recent innovations in computing, however, combined with massive investments in fundamental computing architectures and broadband networks, are ushering in a new era of “online” or “cloud” computing.

Online computing allows users to access IT applications and computing resources over the Internet. This gives users greater choice and flexibility by enabling them to combine the power and reliability of software running on their own PC or other device with the ease and efficiency of computing delivered as a service. While consumers have used online computing for years—through services such as online email, blogging, social networking, and many others—businesses today are also turning to cloud computing to augment their existing IT systems. Many enterprises use online services for business processes such as customer relationship management, video conferencing, and website management, and are likely to rely on cloud computing for a far greater range of services in the future.

When combined with an organization’s own IT system, cloud computing has many potential benefits. Organizations can reduce capital expenditures for hardware and operational expenditures for IT staff and electricity because these are included in the provider’s fee. Cloud applications typically can be implemented quickly and deployed to thousands of users located around the world, enabling organizations to better share information with their employees, customers, and other partners (and governments to better share information with their officers, citizens, and other governments).

In addition, with applications running remotely and data stored offsite, cloud customers can access their data anytime and from anywhere. Organizations have the opportunity to “test drive” new technologies or applications before deciding whether to use them or invest in bringing them in-house. Users also are able to operate more efficiently and at a lower cost by paying only for the services they need, and they can add or reduce computing capacity nearly instantaneously. This is particularly useful for entities that need additional computing capacity only during certain periods, such as the holiday shopping season, or (for governments) around certain regulatory filing dates. It is also useful for smaller organizations, allowing them to tap into supercomputing power and software applications that previously were available only to the largest global companies and institutions.

Like earlier advances in computing, cloud computing can spur economic growth and job creation by helping businesses become more agile and their workers more productive. Cloud computing also has the potential to address pressing social challenges. In healthcare, for example, cloud computing technologies can cut costs, increase efficiency, decrease medical errors, and improve the quality of the care. Similar outcomes will be created in education, workforce training, public safety, and other areas. In education, for example, by tapping into applications and services offered through the cloud, libraries and community centers in underserved communities will be able to access computer power and information that today is financially or geographically out of reach. Cloud computing will also offer school administrations the same cost savings, agility, choice, and access to cutting-edge computing that

are available to other organizations. This will open new opportunities for schools to expand the quality and accessibility of education, particularly in remote and underserved communities. And on the environmental front, consolidated datacenters will help reduce total energy consumption and use renewable and other environmentally friendly energy sources.

To achieve these benefits, however, cloud computing providers must be able to operate datacenters in multiple locations and to transfer data freely among them. This is necessary for several reasons:

- **Reliability.** Enterprises will adopt online computing services only if they are extremely reliable. To provide this reliability, providers need to be able to replicate data and applications across multiple locations. Thus, in the event of a natural disaster or datacenter failure in one location, customers' applications and data will still be available from a different location.
- **Efficiency.** To maximize efficiency, online computing providers need to be able to transfer work loads and data in real time based on needs and available resources. For instance, during the workday in one part of the world, providers must have the ability to shift computing demand to datacenters where it is night (and where the local need for computing is less). The ability to shift data and applications continually among datacenters is also necessary to avoid under-utilization of datacenters, which can significantly drive up overall energy consumption.
- **Performance.** Everyone has experienced the frustration of using an online service that is slow or otherwise experiences delays. Although these delays can have many causes—such as network congestion or slow servers—delays may also result from the fact that the service is being provided from a datacenter that is located far away—a condition also known as latency. The ability to locate datacenters in multiple locations and transfer data between them allows providers to respond instantaneously to fluctuations in demand and thereby to reduce latency and improve performance.

At the same time, to promote trust in cloud computing, providers also must be able to assure their customers that their data will be kept private and secure. Data that cloud computing providers collect, store, and process on behalf of their customers may be personal, confidential, or otherwise sensitive. For consumers, this might include personal emails, photos, or videos, blog postings, or information about their web surfing activities. For businesses, this might include documents or communications that reveal trade secrets, competitively valuable information, and key assets (*e.g.*, price lists, customer contacts, business plans, etc.), while for governments this data might include personal information collected from citizens (*e.g.*, tax records), employee information and communications, or other information that has been entrusted to government. Providers also may collect data such as a name and address, billing and account information, and other personal data when a customer signs up for service and, to manage services effectively and securely, often collect IP addresses, account activity, and similar data. Ensuring the privacy and security of this information is paramount if cloud computing is to reach its true potential.

II. Conflicting Legal Rules Threaten the Growth of Online Computing

The ability of providers to live up to these user expectations regarding the privacy and security of their information is critical, not only for the future of cloud computing, but also to protect fundamental rights of privacy.

As providers process and store greater amounts of user data, however, they face a growing dilemma. Governments, confronted with the challenge of online crime and the use of the Internet in connection with threats to public safety or national security (e.g., cyber attacks or terrorist plots), increasingly are focused on obtaining access to user content and other data held by these providers. Multiple jurisdictions may have interest in a single matter, each seeking access to user information. There are, however, no universally agreed upon rules governing such access by law enforcement. The result is that service providers are increasingly subject to divergent rules and competing assertions of jurisdiction over user content and data. While these rules take many forms, conflicts between them are being felt in two distinct ways:

- ***Conflicting claims of jurisdiction.*** Law enforcement in different countries often follow different rules on the conditions under which they will assert jurisdiction over user data. Some regimes determine that jurisdiction exists only if the data is physically stored in the country, while others assert jurisdiction so long as the service in question is offered there or if the user to whom the data relates resides there. Still others assert jurisdiction so long as the service provider has a place of business in-country, regardless of where the data is located. Each jurisdiction also has its legal standards and process for lawful access demands by law enforcement. Complying with a lawful demand for user data in one jurisdiction may place a provider at risk of violating the privacy or other laws of the jurisdiction where the data actually sit. Also, this global thicket of conflicting rules makes it extremely difficult for providers to give their customers accurate and adequate notice of the conditions under which their data might be accessed by law enforcement.
- ***Inconsistent legal obligations.*** Differences in national rules on such issues as data privacy, data retention, and law enforcement access also create conflicts among substantive legal obligations. For instance, the disclosure of data to one government in response to a demand that is lawful under that country's rules may violate the privacy rules of another jurisdiction. Compliance with the data retention rules of one country may be considered too long in another country and too short in a third. Indeed, given the absence of a broad agreement among countries on data retention and data access, it is plausible that a country could mandate the deletion of data on its own citizens stored in another country, even though that country's laws either permit or require that the data be retained for a longer period. Another example arises in connection with so-called "blocking statutes," which impose civil or even criminal liability on a company if that company complies with warrants, subpoenas, or court orders issued by a second country for access to data. If a company in one country is served with a subpoena for user data located in a second country that has a blocking statute, the company could be forced to choose between refusing to comply with the first country's subpoena (and potentially being held in contempt of court in that country) or violating the second country's blocking statute (and potentially facing penalties in that jurisdiction).

Many governments have attempted to establish procedures to avoid such conflicts, but the mechanisms for doing so have not been successful in practice. In particular, it is not uncommon for a country to have a number of bilateral Mutual Legal Assistance Treaties (MLAT) with other countries. MLATs are intended to provide a government-to-government mechanism for obtaining access to data held in a foreign country. The international judicial process of "letters rogatory" can serve the same function in criminal cases where no MLAT exists, and in civil cases. These procedures, however, almost always are too cumbersome and slow to be useful in fast-moving criminal investigations or other settings. This is particularly true in the context of online crime, in which threats evolve quickly and the conduct and evidence at issue can easily traverse multiple jurisdictions. Also, although nearly four dozen countries have ratified and/or signed the Council of Europe's Convention on Cybercrime, which seeks to expedite

the sharing of evidence on computer crimes, the Convention does not provide a mechanism for resolving competing claims of jurisdiction over data or differences in substantive legal rules.

As a result, law enforcement in certain countries have begun to ignore these established procedures and simply demand that local employees disclose data regardless of where it is located or to which jurisdiction the relevant service is provided—demands that often are backed up by threats of fines or even imprisonment. This places online computing providers in an untenable position. If they refuse to disclose data stored abroad, they face punishment from local law enforcement. If they agree to disclose the data, they face the risk not only of a significant loss of customer trust, but also the potential of liability under the privacy regime or related laws of the jurisdiction where the data is stored. This Catch-22 also can have unintended effects for governments with respect to their ability to access information for law enforcement purposes. Specifically, service providers that are caught in the no-win situation may be slower in responding to governments' requests for access to data as they grapple with what to do and how to strike the right compromise, however unlikely such a compromise may be.

There have been several examples of the serious threats these competing and, at times, conflicting requirements can pose to service providers and the user data they possess:

- **Belgium.** A Belgian criminal court fined Yahoo! nearly \$70,000 for failing to provide Belgian law enforcement authorities with detailed account data for a number of e-mail addresses for Yahoo!'s U.S.-based online email service, Yahoo.com, that allegedly were being used by criminals in Belgium. Yahoo! reportedly argued that because it did not maintain business operations in Belgium, did not direct its services at Belgian users, and did not store the data in question in Belgium, Belgian law enforcement were required to seek such data through U.S. authorities via the MLAT treaty in place between Belgium and the United States. The Belgium court rejected this argument and held that Belgian authorities had jurisdiction over the data. The court also imposed a daily fine of over \$12,000 for each day that Yahoo! continued to refuse to turn over the data.
- **Brazil.** A Brazilian court demanded that Google turn over information related to users of its social networking site, despite the fact that the information was stored in the United States. Google reportedly insisted initially that the Brazilian government go through the U.S. judicial system to obtain the data but nevertheless was ordered to disclose the data to Brazilian authorities or pay a daily fine of \$23,000 for noncompliance.
- **Italy.** Italy imposes a 12-month data retention obligation on online service providers, while some other countries, including some European countries, require that data be retained for a shorter period of time. Some Italian prosecutors have interpreted Italy's data retentions law to apply to data held by U.S. providers even if they do not store data in Italy and have threatened criminal proceedings to enforce compliance with their views.

To encourage continued investment in cloud computing services, there must be greater clarity and consistency on rules that will protect the privacy and security of user data while also ensuring legitimate law enforcement needs are addressed.

III. Industry Efforts to Cope With These Problems

Online computing providers have taken several steps to seek to resolve these dilemmas, or at least lessen their impact. Microsoft, for example, has adopted a policy of responding to law enforcement

demands to block access to Windows Live Spaces content only if it receives official written notice from a government indicating that the material violates local laws. Also, to the extent technically possible, Microsoft will block access to such content only in the country issuing the order while continuing to provide access to users in other countries. The company also informs local users that access to the content was blocked due to a government demand. Other online computing providers have taken similar steps. Google, for example, has a policy of blocking YouTube videos that are clearly illegal in a particular country only to users in that country, but will continue to allow users located elsewhere to access such videos.

Online computing providers also are expending considerable resources to ensure that their physical operations and corporate structure minimize the problems posed by conflicting legal rules—often at the expense of the efficiencies and other benefits cloud computing can provide. But these efforts cannot entirely solve the problem—for both business and technical reasons, it simply is impractical to locate servers in every jurisdiction or to strictly segregate data in multiple locations based on the presumed location of users.

The leading private-sector effort in this area to date is the Global Network Initiative (GNI), which was announced in late 2008 by a coalition of companies, investors, and human rights organizations. The GNI promulgated voluntary guidelines for companies to follow in determining how to respond to government demands for censorship or access to user data. Under these guidelines, participants in the GNI—which include many of the leading global service providers—have agreed to require that governments follow established domestic legal process, and to interpret government restrictions, demands for user data, and jurisdictional claims narrowly so as to minimize the negative effects of such demands on user-generated content.

Despite these important steps, the private sector alone cannot resolve these problems. Companies that are physically present and operating in a jurisdiction have a legal obligation and practical imperative to comply with local law and to accede to local law enforcement demands for user data. Their refusal to do so can imperil their businesses and jeopardize the safety of their employees. These problems will only grow as cloud computing becomes more popular. Failure to resolve them will pose a serious crisis for industry, consumers, and governments alike, and risk the future expansion of the Internet and the vast potential for innovation that is presented by the next generation of computing.

IV. The Need for Government Leadership

While industry must also play its part, any long-term solution to the problem of conflicting jurisdictional claims and inconsistent legal obligations ultimately must involve all stakeholders—and specifically include leadership from governments. Crafting rules in this area undoubtedly poses challenges, but it also presents opportunities, since governments that take the lead in resolving these issues are likely to have a significant advantage in promoting the growth of online computing in their jurisdictions—and reaping the benefits these technologies offer for job creation, productivity, and economic growth. There are several options worth exploring in this regard:

- ***A new multilateral framework.*** One ambitious, but also perhaps most effective, avenue for a solution would be for governments to seek a multilateral framework on these issues in the form of a treaty or similar international instrument. This could include updating an existing treaty (such as the Convention on Cybercrime) or drafting a new one. While this option would undoubtedly require significant diplomatic leadership and resources, it offers perhaps the best hope of addressing

legitimate government needs in a coherent fashion while ensuring that business and consumer interests in privacy and freedom of expression are adequately met on a global scale. To initiate this process, an entity such as the G8 or G20 could take up the issue, then ask the OECD, APEC, or a similar multi-lateral organization to research the problem and make recommendations for how to resolve them.

- **More active bilateral consultations.** A less formal option would be for countries to engage independently in consultations and consensus building on procedures for resolving data access and censorship issues in ways that avoid conflicts. Even bilateral discussions on these issues will increase awareness of the problems created by conflicting claims of jurisdiction and pave the way for a longer-term, more formal solution. The law enforcement and diplomatic community in the United States, EU member states, the Commonwealth countries, and other leading nations could lead such consultations by: (1) engaging with their counterparts in other governments to resolve ongoing issues where laws appear to conflict, with an aim toward creating a lasting solution to systemic issues; and/or (2) signaling to industry a willingness to engage in government-to-government dialog on a case-by-case basis when a company finds itself facing conflicting legal obligations.
- **Enhanced MLATs.** Another option would be for individual governments to press for enhanced MLATs with their MLAT partners. Specifically, MLAT signatories could seek to improve the speed and effectiveness of assistance between them. While it is an open question whether this option could provide a permanent solution to these issues, if such enhanced MLATs were pursued by the United States, EU member states, the Commonwealth countries, and other leading nations, they would at a minimum provide a vehicle for these governments to address the challenges facing service providers in their respective countries.

V. Conclusion

With the growth in online computing, increasing amounts of user data are being processed and transferred across national borders. To take full advantage of online computing, users must be given reliable assurance regarding the privacy and security of their online data, while providers of online computing must be able to offer such assurances without fear of conflicting legal obligations. It is vital that governments around the world engage on this issue and work with industry to adopt harmonized, coordinated rules for access to, and the protection of, online data.

For more information please contact Pamela Passman (ppassman@microsoft.com), Rich Sauer (rsauer@microsoft.com), or Mike Hintze (mhintze@microsoft.com) of Microsoft's Corporate and Regulatory Affairs department or visit www.microsoft.com/publicpolicy.

Microsoft