Microsoft

January 2010

Building Confidence in the Cloud: A Proposal for Industry and Government Action to Advance Cloud Computing

Executive Summary

The rapid growth of cloud computing offers tremendous potential for efficiency, cost savings, and innovation to governments, businesses, and individual users alike. Yet there are several challenges to widespread adoption of cloud technologies. These include legitimate questions about the privacy and security of data stored in the cloud. For the full benefits of cloud computing to be realized, users must have confidence in a cloud that is protected from the efforts of thieves and hackers and that also serves as an open source of information to all people around the world.

Microsoft is responding to this need by working to build more secure systems and datacenters and adhering to clear, responsible privacy and security practices—from software development through service delivery, operation, and support. In order to clear the path for the enormous benefits of cloud computing, government action is also needed to ensure that there is a sufficiently robust privacy and security legal framework to protect and provide user rights and benefits in the cloud.

I. The Promise of Cloud Computing

We have entered a new era in computing, one in which software running on users' own PCs and IT systems increasingly is complemented by applications and services accessed over the Internet from remote datacenters, i.e., "the cloud." The potential benefits of cloud computing are enormous. They include greater efficiencies for organizations to customize and rapidly scale their IT systems for their particular needs, expanded access to computational capabilities previously available only to the very largest global companies, better collaboration through "anywhere, anytime" access to IT for users located around the world, and new opportunities for innovation as developers flock to this latest computing paradigm. For governments in particular, cloud computing offers the potential to reduce costs in a time of economic constraints while making data more easily accessible to citizens and making the process of governance more transparent.

These are among the many reasons why Microsoft is extremely excited about the potential benefits of cloud computing and why we have invested heavily in our cloud infrastructure and the development of products and tools that maximize user flexibility and choice and ensure a seamless computing experience between client devices and the cloud. We are hardly alone in our enthusiasm, with many others in the industry making substantial investments in the cloud.

II. Challenges to the Adoption of Cloud Computing

To realize the full benefits of cloud computing, users must have confidence that any data they create, share, or store in the cloud will be kept private and secure. We are not there yet. The Federal Trade Commission (FTC) recently cautioned that "the storage of data on remote computers may . . . raise

privacy and security concerns for consumers."[1] And the Administration's own Chief Information Officer, Vivek Kundra, has noted that the government will need to "address various issues related to security, privacy, information management and procurement to expand [its use of] cloud computing services."[2]

There are many security experts, including at Microsoft, who note that cloud computing can advance security. Most cloud computing providers have greater security expertise and better security controls than most enterprises and even most government agencies. Yet the aggregation of massive amounts of data in large datacenters also creates a new and highly tempting target for criminals. As criminals turn their attention to these vaults of information—and they will—it will become increasingly challenging to protect such datacenters from both physical and cyber attacks.

There also are privacy implications raised by the cloud infrastructure. The cloud will move data from local on-site PCs and servers to equipment that is physically and administratively controlled by a third party and that may contain information belonging to others. This shift from the desktop to the cloud raises the issue of what the third parties can do with the information and who can access it.

Industry has an important responsibility to pursue initiatives that address the privacy and security risks of cloud computing. Microsoft appreciates this responsibility and the importance of building confidence in the cloud for our customers. For that reason, we constantly are working to improve our privacy practices and strengthen the security of our online services.

The private sector, however, cannot build user confidence in the cloud on its own. The solution requires a cooperative effort from all stakeholders, including governments. While elements of a strong privacy and security framework for cloud computing already exist, many elements of this framework were designed for earlier technologies and leave important gaps in protection.

To ensure that cloud computing reaches its full potential, we need a national conversation on privacy and security in the cloud. This paper is intended to contribute to that conversation.

III. A Call for Responsible Government Action

For the cloud to deliver on its promise, Congress needs to take responsible action to foster users' confidence that their privacy interests will be preserved and their data will remain secure in the cloud. These reforms—which could be combined in a "Cloud Computing Advancement Act"—should:

- ***Strengthen privacy*** by ensuring that users are not forced to give up their reasonable expectations of privacy when they move data to the cloud. Among other things, Congress should update the Electronic Communications Privacy Act and related laws to account for how people use cloud technologies today and how they will use them in the future.

---

[1] FTC, *Comments – NBP Public Notice #21 (Comments to the FCC's Notice Of Inquiry)* (Dec. 9, 2009). The FTC went on to note that "the ability of cloud computing services to collect and centrally store increasing amounts of user data, combined with the ease with which such data may be shared with others, create a risk that larger amounts of data may be used by entities in ways not originally intended or understood by consumers."

[2] Vivek Kundra, White House Blog, "Streaming at 1:00: In the Cloud" (Sept. 15, 2009), available at http://www.whitehouse.gov/blog/streaming-at-100-in-the-cloud/.

- ***Enhance security*** by increasing law enforcement resources and strengthening criminal and civil enforcement mechanisms against malicious hacking of cloud services. As a first step, Congress should amend the Computer Fraud and Abuse Act (CFAA) to make it easier for law enforcement and cloud providers to combat unauthorized access to data stored in the cloud. Congress also should provide law enforcement with the funding it needs to pursue cybercriminals.

- ***Help users make informed choices*** by promoting transparency around cloud providers' security practices.

In addition, the Administration can help ***promote user confidence in the cloud*** by working with other governments to agree on common approaches to jurisdiction over cloud services and data stored in the cloud—an issue that is of particular concern where cloud services cross national borders.

A. Strengthen Privacy Protections by Updating the Electronic Communications Privacy Act

In the United States, any discussion on the right to privacy—including in relation to the cloud—should begin with the Fourth Amendment to the Federal Constitution. In one sense, the migration of data to the cloud does not present a qualitatively new or different issue under the Fourth Amendment: consumers have been sharing and storing data online—through services such as hosted email, instant messaging, and social networking—for years. However, the Fourth Amendment protects against unreasonable search or seizure by the state only of information in which users have a reasonable expectation of privacy, and there are many court cases holding that an individual's reasonable expectation of privacy is greatly diminished when information is shared with a third party. While this constitutional analysis often is highly fact specific and there is no clear precedent fully addressing the various potential uses of cloud computing, it seems clear that at least some uses of cloud computing may not enjoy the same full Fourth Amendment protections that apply to data stored locally.

Ideally, the courts ultimately will decide to extend Fourth Amendment protections to the cloud. In the meantime, however, while the contours of Fourth Amendment protection remain uncertain, some users may be reluctant to transfer their most valuable and confidential data to the cloud. This uncertainty is an obstacle to the full development of the cloud's potential. Congress needs to act to give users confidence that the use of cloud computing will not require sacrificing their privacy. As a first step, Congress should reform the principal statute for protecting user privacy in electronic communications, the Electronic Communications Privacy Act (ECPA).

ECPA was enacted in 1986 to provide a comprehensive privacy framework for data shared or stored in various types of telecommunications services. ECPA grants certain protections to customer data when it is transferred across or stored in such systems and establishes rules that law enforcement must follow before they can access that data. One of ECPA's key goals was to strike a balance between protecting individuals' privacy interests in communications and law enforcement's legitimate need for access to data as part of investigations. Accordingly, ECPA places limits on a service provider's ability to disclose customer data to others, but also sets forth the legal process that law enforcement must follow when they seek to access such data. Depending on the type of customer information involved and the type of service being provided, the required process varies from a search warrant to a subpoena.

However, ECPA has not kept pace with the development of the Internet. While Congress has amended ECPA several times since it was passed, these amendments have not revisited the basic technological assumptions upon which the Act was based or changed the fundamental contours of the protections

afforded to stored electronic communications. As a result, the statutory framework erected by ECPA is built on an antiquated, pre-Web foundation, one that has failed to keep pace with innovations in computing and in how users interact with each other through the Internet.

For example, ECPA classifies all covered services under two definitions, "electronic communications services" and "remote computing services." This definitional question is critical, because how a service is classified under the law has a major impact on the process by which law enforcement can access customer data held by such services. Due to the transformative changes in computing and the Internet since 1986, however, these definitions are no longer sensible, or even intelligible—especially as they apply to providers of cloud services. As a result, cloud service providers (as well as law enforcement and the courts) are faced with the increasingly challenging task of determining which provisions of ECPA apply to any given online service.

As another example, ECPA today extends greater privacy protections to emails stored for less than 180 days than emails stored for more than 180 days. These distinctions might have made some sense in 1986, when email services did not automatically retain messages for long periods of time. But that distinction no longer bears any relationship to reality—hosted email and other online services almost invariably store emails and other content for years, and users reasonably expect these communications to remain just as private on day 181 as on day 179.

In short, ECPA has been overtaken by technological change, and it no longer strikes the right balance between consumers' privacy interests and the government's legitimate need to access user information. This needs to change.

For these reasons, Microsoft supports the efforts to modernize ECPA that are being led by the Center for Democracy and Technology (CDT). We believe such reform is vital to bring the statute up-to-date and into alignment with current technological realities.

These reforms of ECPA would complement prior calls for an omnibus federal privacy law, which Microsoft has supported. An omnibus law would ensure that consumers understand and have control over the data collected about them both online and offline. In combination, omnibus federal privacy legislation, responsible reforms to modernize ECPA, and industry leadership and best practices can help create an environment that addresses users' legitimate concerns over the privacy implications of cloud computing and engenders user confidence in the cloud.

B. Deter Malicious Hacking of Cloud Services

Microsoft has a long history of supporting law enforcement to help fight digital crime. In our experience, three elements are critical to combating digital crime successfully: (1) strong deterrence through criminal and civil enforcement with meaningful penalties and remedies; (2) a legal framework that encourages cooperation and information-sharing between the public and private sectors, especially the sharing of technical expertise; and (3) the ability for law enforcement in different jurisdictions to team up and share information globally. Our proposal in this paper focuses on the first element: strong enforcement tools.

Today, one of the principal tools for combating digital crime in the United States is the Computer Fraud and Abuse Act (CFAA). The CFAA has proven to be an effective weapon in the fight against digital thieves, fraudsters, and malicious hackers. Among other things, the statute prohibits obtaining

information through unauthorized access to a computer or access to a computer in excess of authorization. 18 U.S.C. § 1030(a)(2)(C). This "unauthorized access" provision is sufficiently broad to cover malicious hacking of online services. The challenge, however, is establishing the aggravating factors under the statute that trigger felony penalties of up to five years in prison and up to a $250,000 fine. These penalties require prosecutors to establish difficult-to-prove elements, such as that the offense was committed for commercial advantage or private financial gain; was committed in furtherance of a criminal or tortious act in violation of U.S. or state law; or the value of the information obtained exceeded $5,000.[3]

To provide law enforcement with the tools it needs to pursue malicious actors, Congress should amend the CFAA in at least two respects:

- First, Congress should establish presumed losses attributable to unauthorized access to accounts hosted online. Specifically, the CFAA should be amended to state that, for purposes of establishing the thresholds necessary to impose felony penalties (*e.g.*, that the value of the information obtained exceeds $5,000 under § 1030(c)(2)(B), or that the value of information obtained through fraud was over $1,000 under § 1030(a)(4)), prosecutors can establish this value by multiplying a specified statutory amount (such as $500) by the number of violations, where each separate account accessed without authorization would amount to an additional violation.

- Second, Congress needs to amend the CFAA's penalty provisions to ensure that the penalties for maliciously hacking into a single cloud datacenter correspond to the number of user accounts illegally accessed and are not subject to the same limits that apply to a person who hacks into a single PC (currently $250,000). Accordingly, the CFAA should be amended to make clear that a separate violation occurs for every individual or business whose information is accessed (i.e., $250,000 per user account illegally accessed). Such an amendment will enable prosecutors to secure larger penalties for hackers that access cloud computing infrastructure.

The private sector also can do its part to deter cybercrime by bringing civil actions against violators. The CFAA currently provides a cause of action for any person who suffers damage or loss as a result of a CFAA violation. However, only a person who actually suffers damages or loss as a result of a violation may sue under this provision. In many cases, this will preclude cloud service providers from instituting such actions on behalf of their customers.

Accordingly, Congress should amend the CFAA's civil action provision to make clear that cloud service providers have a private right of action against those who illegally access their datacenters or gain unauthorized access to the accounts of their customers. This cause of action, much like similar provisions under the CAN-SPAM Act, would bring more private-sector resources to bear against malicious hackers by authorizing cloud service providers to pursue digital criminals on behalf of their

[3] Absent any aggravating factors, a violation of § 1030(a)(2)(C) is a misdemeanor punishable by a fine or imprisonment for not more than one year, or both. As a Class A misdemeanor that does not result in death, 18 U.S.C. § 3571 limits the maximum fine to $100,000.

customers. Further, Congress should provide meaningful statutory damages for successful civil actions, rather than requiring plaintiffs to prove economic damages as is the case under the CFAA today.

These amendments to the criminal and civil provisions of the CFAA should be buttressed by the appropriation of additional resources dedicated to federal law enforcement for cybercrime investigation and prosecutions. The need for enhanced law enforcement training, the development of expert forensic analysis related to computer crimes, and resources to combat cybercrime is greater than ever. The ability to identify perpetrators of online attacks is one of the most fundamental challenges facing the international law enforcement community today. It is a challenge that will only increase as more data moves to the cloud. Vigilant, well-trained law enforcement personnel and sophisticated forensics capable of keeping up with evolving threats are critical to enhancing the security of the online environment and to realizing the full capability of cloud computing.

C. Enhancing Security through Greater Transparency

Cloud providers differ in important ways in their approaches to security. These differences spring from various factors—differing business and revenue models; whether the provider traditionally has focused more on consumer as opposed to enterprise or government customers; differing assessments of how best to mitigate and manage security risks; and other factors particular to that cloud service provider. The fact that security approaches vary is not inherently problematic. On the contrary, this variation may provide one important way in which cloud service providers can differentiate their offerings with potential customers.

Unfortunately, in today's marketplace, the distinctions between cloud providers' security practices are virtually invisible, in practical terms, to customers of cloud services. All providers claim that their systems are secure, but few back up these claims with the specifics that enable users to evaluate these claims or to compare vendors' security practices in any meaningful way. This lack of transparency is undoubtedly one of the main reasons technology officers both within the government and at major corporations express serious concerns about cloud security. Users need more and better information to make informed decisions about the use of cloud services.

This obstacle is surmountable, but it requires action by both the public and private sectors. Cloud providers, for their part, must work to be more informative about their actual security practices, so that users can make educated decisions about their options. Cloud providers also should engage with other stakeholders, such as representatives of consumers, on how best to educate users on security. There should be ***transparency*** over how data is protected, and there should be ***flexibility and choice*** for all users to make informed decisions about the best deployments of cloud services. There are certain fundamental elements—or "truth in cloud computing" principles—that would enable users to make such informed decisions. These include transparency with respect to whether the architecture, infrastructure, and related information security controls of service providers satisfy well-recognized and verifiable security criteria; whether service providers use appropriately robust authentication mechanisms in light of the services and level of sensitivity of the data at issue; and the extent to which applications and other components of cloud services receive strong security testing before deployment. ***Simply put, it should not be enough for service providers simply to say that their services are secure; there needs to be some transparency about why they are secure***.

One approach to achieve this objective would be for industry to adopt a new self-regulatory code. However, Congress may also play a constructive role. Specifically, if there is to be a law in this area, we

believe that all stakeholders—including both industry and users—would benefit if that law were adopted at the federal level and constructively promoted transparency. Such "*Truth in Cloud Computing"* provisions could be part of the Cloud Computing Advancement Act and administered by a federal agency, such as the Federal Trade Commission. One constructive way to help promote transparency would be to require cloud providers to maintain a comprehensive written information security program, one that provides safeguards appropriate for the use of the services, and to disclose to customers a summary of this program. For example, service providers could be required to state whether their information security programs comply with leading third-party standards, such as the International Standards Organization series (27000) for information security management, the Federal Information Security Management Act, or similar requirements; whether they utilize appropriately robust authentication mechanisms; and whether applications and other components of the service (both hardware and software) receive thorough security testing before deployment.

Government agencies also can help promote security and competition by taking into consideration their own security risk profiles; conducting due diligence on service providers with this risk profile assessment in mind and selecting services that best fit their needs in light of agencies' risk profile; and ensuring that all procurement of cloud services occurs in a fair, open, and transparent manner that allows all vendors to compete on a level playing field.

D. Promote User Confidence in the Cloud through Common Approaches to Jurisdiction

As the cloud evolves, and as providers begin to process and store greater amounts of user data, 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, increasingly are focused on obtaining access to user content and other data held by cloud service providers. Multiple jurisdictions may have an 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, and at times conflicting, rules governing jurisdiction over user content and data. Further complicating the problem is the fact that different jurisdictions also have different laws regarding privacy rights and data retention.

This global thicket of competing and conflicting laws presents a significant obstacle to the delivery of cloud services that meet users' reasonable expectations of privacy. Where the rules of different nations conflict, a cloud provider's decision to comply with a lawful demand for user data in one jurisdiction may place a provider at risk of violating the privacy or other laws of another jurisdiction. Equally troubling, this situation 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.

Many governments have attempted to establish procedures to avoid such conflicts, but the mechanisms for doing so have not been successful in practice. International legal instruments for the sharing of information have proven slow and cumbersome, and they have encouraged some countries to begin to ignore 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. 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.

To achieve this objective, governments can take several steps. One ambitious, but also the 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. 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.

A less formal option would be for countries to engage independently in consultations and consensus building on procedures for resolving data access 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. This approach could be complemented by a push for enhanced mutual legal assistance treaties, which could, in turn, help harmonize domestic legislation regarding data privacy issues.

Whatever option governments take, it is absolutely essential that these deliberations include not only representatives from law enforcement and justice, but also representatives of industry, consumer groups, and other interested stakeholders. Cloud computing will only reach its full potential if providers can establish datacenters and offer services in multiple jurisdictions, without fear that each step will invite competing claims of jurisdiction and government access to data. The rules must balance the legitimate needs of law enforcement, industry, and users, and it is vital that all stakeholders are represented in any deliberations.

* * *

One reason that personal computers revolutionized the home and workplace was that PCs empowered consumers and businesses. PCs provided users with rich new experiences and ways to connect and conduct business, while still staying in control over their information. Because the technology and the accompanying legal regime left people in control of their information, they were not forced to make a trade-off between flexibility and efficiency on the one hand and privacy and security on the other.

As we enter this new era of cloud computing, it is imperative that consumers, business, and governments have cause for confidence in the cloud. While industry must take the lead, governments too have a critical role to play. Specifically, they should work to bring existing legal frameworks up-to-date and into alignment with current technology.

With the benefit of a modernized regulatory framework, industry will have the solid grounding to deliver on the promise of cloud computing and once again expand the boundaries of innovation. Microsoft is committed to being part of this effort and looks forward to working with other stakeholders to achieve these goals.

For more information please contact publicpolicy@microsoft.com or visit
www.microsoft.com/publicpolicy.

Microsoft