Microsoft

Trustworthy Computing

Building Global Trust Online

Policy Perspectives on Privacy, Security, and Safety

Advances in computing and communications technologies

have made our lives more connected and more convenient than ever before. Online services now span across many aspects of everyday living, including: business, education, communication, government, and social advocacy. While these innovations provide many distinct advantages, the complex and interconnected systems that have been developed to provide such services – and the massive databases and technological infrastructures that maintain billions of public and private records – present new and unique challenges.

Privacy and safety often top the list of concerns for policymakers and individuals the world over, as technological tools created for the betterment of society are likewise being used as instruments for crime and malicious intent. Criminals and irresponsible businesses are a serious cause for concern among individuals, large organizations, and governments.

Growth and innovation in global computing depend upon a trusted online environment that allows people to use the Internet with a sense of confidence and control over how their personal information is stored and used. At Microsoft, our vision means that we strive to develop products and services that ensure a safer computing experience – while recognizing that the safety and privacy issues of a global online Internet are larger than any one organization can single-handedly address.

The issues of safety, security, and privacy are complex and changing, and they require an ongoing, multi-faceted response to develop effective solutions. Microsoft is committed to sharing information, technology, and experience through collaborations across industries and geopolitical boundaries to make the Internet safer.

The materials in this booklet are a starting point. On the following pages you'll find overviews of key issues; a summary of Microsoft's response to these issues, which includes products, services and global collaborations; and a list of helpful resources and links for further reading and support. This information has been drawn and compiled from extensive work and ongoing research by Microsoft's internal teams, as well as external subject-matter experts.

We've provided information about topics such as:

Current online privacy issues and practices

Issues related to the protection of youth online

Current efforts and resources used to address, mitigate or resolve today's cyber threats

Microsoft's products, services, partnerships, and ongoing work to promote a safer Internet

This booklet is intended to be a relevant and useful guide for any decision-maker with responsibility for developing new ideas and solutions for online privacy, security, and safety. We appreciate the scope and changing complexities of these issues – as well as the tremendous value of collaborative efforts to provide the most up-to-date information, support, and guidance.

We support a global sharing of knowledge and expertise. In fact, our efforts to compile and update these documents would not be possible without the feedback and support of government leaders and policymakers, privacy advocates, our global partners, leading industry experts, and millions of Microsoft customers and other computer users worldwide. By further developing and supporting global partnerships, we can better assist policymakers, organizations, and consumers who must make prompt, relevant decisions about their privacy and safety online.

As with any publication with an intended global audience, we provide this information with the understanding that every region will have different priorities, concerns, and ideas for solutions. That's why we support an open exchange of ideas and information to develop effective global policies and practices – and we recognize that solutions must be widely socially acceptable and meet with public approval, especially with regard to balancing security and privacy.

We live in an increasingly interconnected world – often described as a world of digital dependence – which presents new challenges and concerns that cannot be met or addressed in isolation. That's why we favor solutions made in collaboration, not isolation, and why we continue to call for a coordinated and sustained effort across all affected societies worldwide.

We believe that industry cooperation with authorities is the most effective means of reducing overall cyber threats, and we support balanced regulation as part of that effort. We also support a multi-faceted approach to data governance that involves a combination of policy, people, processes, and technology to create a more trusted personal computing experience and a safer, more secure Internet for everyone.

What's inside

Security

Privacy

Safety

Microsoft Trustworthy Computing

March 2011

Background

The Internet allows people to enrich their lives, build commerce, and facilitate communication around the globe. At the same time, the more people connect online, the greater the need to understand the implications of online security, safety, and privacy.

Microsoft's approach is called Trustworthy Computing, a long-term, collaborative effort to create and deliver secure, private, and reliable computing experiences for everyone. We are committed to continually improving trust by focusing on four key areas: security, privacy, reliability, and business practices. As the Internet becomes increasingly critical to daily life, we are, also advancing End to End Trust, our vision for a safer, more trusted Internet.

Microsoft is committed to helping create a safer, more trusted Internet. We believe fundamentally that sensitive data and personal information must be protected. We believe that technology should adhere to business practices that promote trust. We act according to the principle that the technology industry should focus on solid engineering and best practices to ensure the delivered products and services are more reliable, secure, and trusted. We support collaboration of technology companies, governments, consumers, and businesses to solve the security challenges of today and tomorrow.

Security

At Microsoft, we focus on innovation in secure software development. The Microsoft Security Engineering Center (MSEC) helps to protect Microsoft customers by delivering more secure products through the Microsoft Security Development Lifecycle (SDL), a process that creates software that is less vulnerable and more resilient to malicious attacks. We share our security development methods and processes with others in the industry to promote trusted computing. Our Security Science team performs research that helps us and our customers understand online attacks and techniques. For Microsoft products and services, Microsoft addresses threats and vulnerabilities through two additional centers. The Microsoft Malware Protection Center (MMPC) analyzes malicious software and develops solutions that are used in Microsoft security technologies. It also produces the Security Intelligence Report, an in-depth review of trends in the malicious and potentially unwanted software landscape. In the event a vulnerability is discovered, the Microsoft Security Response Center (MSRC) monitors the situation and responds to the incident. It also manages the company-wide security update release process, and serves as the single point of coordination and communications for these matters.

Helpful Resources

www.microsoft.com/security
Microsoft Security

www.microsoft.com/twc
Trustworthy Computing

www.microsoft.com/endtoendtrust
End to End Trust

www.microsoft.com/sdl
Security Development Lifecycle:

www.microsoft.com/mmpc
Microsoft Malware Protection Center

www.microsoft.com/msrc
Microsoft Security Response Center

www.microsoft.com/sir
Microsoft Security Intelligence Report:

www.microsoft.com/privacy
Microsoft Privacy

Privacy

Microsoft regards protecting privacy as a foundation of trust, and it regards customer trust as critical to the success of our business. People and businesses must have control of their information and how it is used. Microsoft was one of the first companies to appoint a chief privacy officer more than 10 years ago, and today more than 40 Microsoft employees work on privacy full-time. Meanwhile, hundreds more at the company help to ensure that privacy policies and technologies are applied across our products and services. For consumers, we provide privacy-enhancing technologies in our products and services that assist in protecting their personal information. To help organizations more effectively manage the data in their possession, we provide guidance, frameworks, and technologies designed to help protect and manage personal information, mitigate risk, achieve compliance, and promote trust and accountability.

Reliability

Cloud computing can provide substantial cost and efficiency benefits and deliver the latest tools and technology more easily. However, with the rise of the cloud, reliability becomes even more critical. If cloud computing is to fulfill its promise, online services must be as or more available and resilient than their server and desktop counterparts. Microsoft is driving cloud computing reliability by reengineering key products such as Microsoft Exchange Server and Microsoft SharePoint® Server to work better as cloud services, and by implementing cutting-edge data protection and robust service redundancy in online services data centers.

Policy Considerations

Microsoft believes public and private partnerships are also essential to address the increasing complexities of cyber crime—we can't do it alone. Microsoft works with law enforcement agencies by providing them with technical training and in the development of new technology tools to combat cyber crime. We've also assisted in helping to protect consumers and via legal action to stop cyber criminals. For example, the groundbreaking legal and technical efforts led by Microsoft, in cooperation with academic and industry experts around the world, worked to shut down the notorious Waledac and Rustock botnets, networks of tens of thousands of computers hijacked to spread malware, send spam, and commit other forms of cyber crime.

Key Points

- Microsoft is committed to helping create a safer, more trusted Internet. Our approach is called Trustworthy Computing, a long-term, collaborative effort to create and deliver secure, private, and reliable computing experiences for everyone.
- We believe that technology should adhere to business practices that promote trust. We act according to the principle that the technology industry should focus on solid engineering and best practices to ensure the delivered products and services are more reliable, secure, and trusted.
- We support collaboration of technology companies, governments, consumers, and businesses to solve the security challenges of today and tomorrow. Even parents need to be aware, taking steps to help ensure family online safety, including the use of safety settings.

Botnets

November 2010

Background

A botnet is a network of compromised computers that can be illicitly and secretly controlled by an attacker and then used to perform a variety of illegal actions. Computers in a botnet, called nodes or zombies, are usually ordinary computers sitting on desktops in homes and offices around the world.

A computer becomes a node on a botnet when attackers manage to compromise and install malware on a computer, often by exploiting vulnerabilities in the software running on the computer, or by using social engineering tactics to trick users into installing botnet malware by convincing a user to click on a phony link.

The owners of infected computers are usually unaware that their computers are being used for malicious purposes. When a computer has been infected by botnet malware, the botnet owner secretly connects the computer to the botnet and uses it to perform tasks such as sending spam, hosting or distributing malware or other illegal files, or attacking other computers.

Botnets pose a more dangerous threat than traditional hackers to the information technology systems of enterprise and governments because of the ability of botnets to harness large numbers of individual computers to direct an attack. The raw computing power of a botnet can enable them to take down major websites, email servers, and other essential parts of a critical infrastructure provider's communications, data, and electronic systems.

Microsoft Approach

- At Microsoft, we're determined to help fight cyber crime through legal action, technology, and consumer education.
- Microsoft supports governments and law enforcement by providing them with technical training, investigative and forensic assistance, and the continued development of new technology tools to combat cyber crime.
- The Microsoft Digital Crimes Unit and its partners are taking an aggressive approach in the fight against botnets to make the Internet safer for everyone.
- Using both legal and technical action, Microsoft and industry and academic partners shut down the Waledac botnet in 2010 in an operation that can serve as a model for other actions.
- Microsoft believes in working closely with law enforcement in combating botnets and that public-private partnerships are essential to address the increasing complexities of cyber crime—no one can do it alone.

Helpful Resources

www.support.microsoft.com/botnets
The Microsoft security and safety website

www.microsoft.com/security/
Microsoft Security Essentials, free security software

www.microsoft.com/security_essentials/
Microsoft Update service providing updates to Windows and other components

www.update.microsoft.com
Information on how customers can help clean botnets off their systems

Guidance for Consumers

If you believe your PC may have been infected by a botnet or other malware, Microsoft can help you diagnose the problem and solve it.

Defend your computer with firewall and antivirus software. Keep all software current, including your web browser, with automatic updates. Never turn off your firewall and use thumb (or flash) drives cautiously.

Don't be tricked into downloading malware. Be very cautious about opening attachments or clicking links in email or instant messages, or in messages on social networks. Don't let attackers scare you into action with fake warnings that your computer has a virus or that your bank account is about to be closed if you don't click the button or link they supply. Only download software from websites you trust.

Guidance for Governments

- Microsoft welcomes the support of governments in fighting botnets and other threats. We believe cooperation with authorities is the most effective means for reducing cyber threats in general, and we support balanced regulation as part of that effort. We believe that less onerous restrictions on industry allow for greater innovation and flexibility in implementing responses to cyber crime.
- Microsoft has joined with industry partners to encourage countries to adopt and ratify the Council of Europe Convention on Cybercrime, which requires signatories to adopt and update laws and procedures to address crime in the online environment.

Key Points

- Botnets are networks of compromised computers controlled by remote attackers in order to perform such illicit tasks as sending spam or attacking other computers.
- Botnets are of concern to governments and businesses because of their ability to harness large numbers of individual computers to direct an attack against information technology infrastructure.
- Microsoft is taking an aggressive approach to fighting botnets by collaborating with governments and others to take them down. Microsoft is also providing businesses, governments, and consumers with security tools and guidance.
- Consumers can help protect themselves by strengthening the security of their computers and by training themselves to act defensively as they click their way across the web.
- Governments can help by partnering with industry to take down botnets, and by passing thoughtful balanced regulation.

Critical Infrastructure Protection

February 2011

Background

Governments are increasingly focused on the role critical infrastructures play in supporting the overall economy and security of their nations. Critical infrastructures are generally thought of as the key systems (and the services and functions they provide) that, if disrupted, would have a debilitating impact on public health and safety, commerce, or national security.

Advances in software, communications, and IT services have substantially improved and connected these key systems, but their interconnectedness is also a cause for growing concern. Critical infrastructures are attractive targets for criminals, and increasingly sophisticated attacks on interconnected systems have the potential to cause widespread damage and disruption.

The unique security challenges of complex critical infrastructures require an unprecedented response. Technology vendors, governments, businesses, and consumers must work together to innovate, develop, and deploy effective solutions. Microsoft is committed to supporting partnerships and plans to help preempt, detect, and identify the sources of critical infrastructure threats. We formed the Microsoft Global Security Strategy and Diplomacy (GSSD) team as part of that commitment, and we continually work to protect critical infrastructures by increasing the trustworthiness of software and IT services—and by collaborating with governments and critical infrastructure owners and operators to reduce and manage risks.

Microsoft Approach

Microsoft's Global Security Strategy and Diplomacy team is dedicated to addressing the unique challenges of critical infrastructures. Our goal is to drive change that will enhance their security and resiliency, and we can achieve that by building trust, developing innovative solutions, and working with government, industry partners, and critical infrastructure providers. Effective critical infrastructure protection efforts fall within three areas:

- **Trustworthy plans and policies** – Clear, effective policies lead to well-defined goals and priorities that help IT professionals secure resources and focus investments on top priority risks. We collaborate to develop effective, flexible, and innovative national and global solutions to effectively secure infrastructure.
- **Resilient operations** – We can reduce the impact of disruptions in critical infrastructure by sharing best practices and creating a cohesive front when disruptions occur. Greater resiliency will allow IT professionals to manage their environments with greater confidence and more knowledge.

Helpful Resources

www.microsoft.com/sdl
The Microsoft Security Development Lifecycle (SDL)

www.microsoft.com/security/msrc/default.mspx
Microsoft's Security Response Center

www.microsoft.com/msrc
Microsoft's Security Cooperation Program

www.icasi.org
Sharing information

www.safecode.org/
Software Assurance Forum for Excellence in Code (SAFECode)

- **Innovative investments** – Continuous innovation leads to advanced security capabilities, and innovative environments allow IT professionals and organizations to benefit from new thinking, improved products—and better processes, guidance, and training. Microsoft supports collaborative efforts to develop innovative practices, programs, education, and research to develop secure solutions for critical infrastructures.

Policy Considerations

Today's policymakers are tasked with understanding the complex relationships, mechanisms, and frameworks of critical infrastructures and addressing issues that arise from rapid advances in computing and communications technologies. Leaders worldwide are concerned about the security implications of increasingly interrelated global systems, especially economic stability, climate change, and national security. We have seen the potential for disruptions of critical infrastructure to cause unprecedented, widespread damage (similar to the recent global financial crisis). These issues pose daunting challenges for those who must predict and manage their outcomes, and they require a united response from governments and businesses. Innovative public-private partnerships must develop robust plans to secure and protect our critical infrastructures from ever-changing threats and sophisticated attacks. Solutions include:

- **Better, more secure development** – using proven, effective processes similar to the Microsoft Security Development Lifecycle
- **A unified response** – supporting partnerships and investments that identify assets and manage critical function risks
- **Shared information and tested response mechanisms** – helping governments and critical infrastructure operators maintain situational awareness and respond quickly to prevent, mitigate, and recover from nationally or globally significant threats
- **Next generation network technologies** – deploying secure cutting-edge solutions to increase communications capability and resiliency
- **More security research** – solving existing problems and preparing for future problems by strengthening the pipeline of academic and professional knowledge (educating, mentoring, and training future professionals and leaders)

Key Points

- National security and international policy concerns about critical infrastructure have evolved as key systems of public life, health, and safety have become increasingly interconnected and dependent on IT infrastructure.
- The unique security challenges of complex critical infrastructures require an unprecedented response. Technology vendors, governments, businesses, and consumers must work together to innovate, develop, and deploy effective solutions.
- Microsoft's Global Security Strategy and Diplomacy (GSSD) team partners with national governments, multilateral organizations, industry partners, and non-profit organizations to strengthen and improve cyber security, promote trustworthy plans and policies, and help protect key processes and functions for national and economic security, public health, safety, and public confidence.

Cyber Security

March 2011

Background

Governments, industries, and consumers rely on globally connected networks and cyber systems, and create and electronically store enormous volumes of sensitive data. Such data, particularly when not well secured, presents an attractive target for those seeking competitive or strategic advantage—or financial gain.

The resulting cyber crime economy is complex, sophisticated, and growing. Some of its participants are willing, such as malware developers; and some are unwilling, such as unwitting victims of cyber attacks. Those who study vulnerabilities include legitimate security researchers who responsibly disclose vulnerabilities, and vulnerability traffickers who profit from cyber crime. Over the past decade, cyber crime attacks have also grown in sophistication, expanding from opportunistic, disruptive, and damaging viruses and worms to targeted, stealthy, and persistent attacks.

In today's evolving cyber crime economy, any individual can engage in activities formerly limited to nation states, and any nation, regardless of traditional measures of sophistication, can gain economic and military advantage through cyber programs. As a result, cyber security has become a key policy issue, as governments look to protect the confidentiality, integrity, and availability of sensitive information, government services, and critical infrastructure.

Cyber security is a responsibility that governments, businesses, and individuals must share. An effective approach requires collaborative risk management activities between public entities and private sector owner/operators of infrastructures to properly identify threats, vulnerabilities, and consequences and achieve acceptable risk levels—not only for health, safety, and security, but also for business risks.

Microsoft Approach

- Microsoft is a global information technology company whose scale and experience with governments around the world has facilitated expertise and a sophisticated understanding of the changing nature of cyber threats and the challenges that governments face. Microsoft Windows-based software is the most widely deployed platform in the world serving consumers, businesses, and governments.
- Microsoft plays an important role in the online world by providing software and services for hundreds of millions of computer systems worldwide. With more than 15 years of experience, we operate one of the largest online email systems, with hundreds of millions of active email users in more than 30 countries.
- Microsoft's Windows Update Service provides software updates for more than 600 million computers worldwide, and our Malicious Software Removal Tool cleans roughly 450 million computers each month.

Helpful Resources

www.microsoft.com/gssd
Microsoft Global Security Strategy and Diplomacy (GSSD) website

www.microsoft.com/security/gssd/
Microsoft Security Response Center (MSRC) website

www.microsoft.com/sir
Microsoft Security Intelligence Report website

www.microsoft.com/sdl
Microsoft Security Development Lifecycle (SDL) website

www.safecode.org/
Software Assurance Forum for Excellence in Code (SAFECode)

- Microsoft works with the global community to help create a safer, more trusted Internet through our Collective Defense efforts, which strengthen the security of products, services, and devices.
- Microsoft's Global Security Strategy and Diplomacy (GSSD) team partners with national governments, multilateral organizations, industry partners, and non-profit organizations to enhance the security of the Internet, promote trustworthy plans and policies, and help protect key processes and functions important to national and economic security, public health, safety, or public confidence.
- Microsoft is actively involved in industry efforts to develop best practices for IT supply chain risk management and product assurance. Microsoft is an active participant in the Software Assurance Forum for Excellence in Code (SAFECode), a global, industry-led effort to identify and promote best practices for delivering more secure and reliable software, hardware, and services.
- The Microsoft Security Development Lifecycle (SDL) is a security assurance process focused on software development. The SDL contains a collection of mandatory security activities, grouped by the phases of the traditional software development life cycle (SDLC).
- The Microsoft Security Response Center (MSRC) employs some of the world's leading experts on computer security. When a security threat arises, MSRC researchers analyze the risk and distribute security updates. The MSRC also helps customers prioritize their response to new threats.

Policy Considerations

- Microsoft believes that public-private partnerships are the most effective means of identifying and managing strategic and operational cyber security risks. Such partnerships should be built on trust and focused on achieving concrete objectives.
- Microsoft welcomes the support of governments in reducing cyber security threats. We believe that cyber security depends on collaboration and cooperation between government and industry.
- Creating a safer, more trusted Internet is a long-term commitment and a shared responsibility that is often stifled by regulation, and it requires a unified approach by governments, industry, and consumers.

Key Points

- Cyber security is a critical policy concern for governments, industries, and consumers around the world as organizations and individuals increasingly rely on software and services for essential operations.
- An effective approach to cyber security requires collaborative risk management activities between public entities and the private sector in order to properly identify threats, vulnerabilities, and consequences and to achieve acceptable risk levels—not only for health, safety, and security, but also for business risks.
- Microsoft works with the global community to help create a safer, more trusted Internet by constantly improving the security of our products and services, developing best practices, and collaborating to reduce cyber security threats.

Data Breach Notification

March 2011

Background

In recent years, media reports about data breaches at major public and private institutions have captured both headlines and public attention, especially when those security breaches jeopardized sensitive personal or financial information of millions of private citizens. Data breaches not only put consumers at risk of fraud and identity theft, but they also jeopardize the relationship between consumers and historically trusted organizations or government infrastructures. Organizations that embrace key concepts of data governance can reduce the risk of data breaches and develop effective plans to address security issues when they do occur.

Governments at all levels are examining the need for legislation that governs data breach notification policies, which require companies or agencies to notify customers when their personal data has been put at risk or compromised. Current laws usually take one of two forms: acquisition-based trigger legislation, or risk-based trigger legislation.

Acquisition-based trigger legislation requires an organization to notify affected individuals whenever personal information has, or can reasonably be assumed to have been, acquired by an unauthorized person. Risk-based trigger legislation requires an organization to notify affected individuals only when a significant potential risk has been identified.

As policymakers have begun to develop legislation governing data breach notification policies, many organizations have responded by adopting more secure technology practices, such as encryption. In fact, in some jurisdictions, organizations are exempt from certain disclosure requirements if their data is encrypted at the time of a security breach. This "encryption exemption" is a powerful motivator for companies to adopt encryption methods and procedures for protecting sensitive data.

Microsoft Approach

Microsoft recommends a multi-faceted approach to data governance that involves a combination of policy, people, processes, and technology. Our approach includes creating or maintaining:

- **More secure infrastructure** – with safeguards that protect against malware, intrusions, and unauthorized access to personal information, and protect systems from evolving threats
- **Identity and access control** – with systems that help protect personal information from unauthorized access or use and provide management controls for identity access and provisioning
- **Information protection** – by securing sensitive personal information in structured databases and protecting unstructured documents, messages, and records with methods such as encryption
- **Auditing and reporting** – by monitoring to verify the integrity of systems and data in compliance with business policies

Policy Considerations

- In many countries and regions, conflicting laws complicate the process of compliance across local, state/provincial, or international borders. The wide variances in rules, regulations, and laws threaten to impede economic progress and stifle innovation. In countries such as the United States with multiple state laws, Microsoft supports broad federal preemption as part of any comprehensive privacy legislation. Policymakers, industry, and organizations must work together to develop a mutually agreeable, effective solution that protects both privacy and innovation.
- Microsoft supports data breach notification legislation that includes:
  - » an acquisition-based trigger of notification when data containing personal information is acquired by an unauthorized person and a significant risk of fraud or identity theft can reasonably be inferred;
  - » a requirement to notify those who are affected within a reasonable time period, unless otherwise directed by a law enforcement agency pursuing an investigation;
  - » a 45-day grace period before notifying consumers so an organization can have time to investigate and mitigate data breaches by securing their systems and networks.

Helpful Resources

www.microsoft.com/privacy
An overview of Microsoft privacy policies and initiatives

www.microsoft.com/datagovernance
Microsoft's Data Governance website

www.microsoft.com/sdl
Microsoft's Security Development Lifecycle website

Key Points

- Data breaches put consumers at risk of fraud and identity theft and jeopardize the relationship between consumers and historically trusted organizations or government infrastructures.
- Microsoft recommends a multi-faceted approach to data governance that involves a combination of policy, people, processes, and technology. Our approach includes creating or maintaining more secure infrastructure, identity and access control, information protection, and auditing and reporting.
- Microsoft supports data breach notification legislation that includes: an acquisition-based trigger of notification when data containing personal information is acquired by an unauthorized person and a significant risk of fraud or identity theft can reasonably be inferred; a requirement to notify affected individuals within a reasonable time period unless otherwise directed by a law enforcement agency pursuing an investigation; and a 45-day grace period before notifying consumers, which gives an organization time to investigate data breaches and mitigate them by securing their systems and networks.

Microsoft End to End Trust

March 2011

Background

The Internet allows people to use tools that enrich lives, build commerce, and facilitate communication around the globe. At the same time, the more people connect online, the greater the need to understand the implications of online security, safety, and privacy. Microsoft's Trustworthy Computing Initiative and the vision of End to End Trust helps provide context for policymakers worldwide who are working to develop cyber security policies and initiatives.

Microsoft is committed to sharing insight and guidance with decision-makers and public policy leaders to help define priorities and take substantive action to ensure secure online practices. End to End Trust can be realized by focusing on three key areas:

- **Security and Privacy Fundamentals** – A trusted online environment relies on technology that is built from the ground up with security and privacy in mind, and the core principles of privacy and security should be applied to information technology.
- **Technology Innovations** – End to End trust requires an environment in which reasonable and effective trust decisions are made. This environment depends on a "trusted stack" comprising security rooted in the hardware, trusted software, trusted data, and trusted people.
- **Social, Economic, Political and IT Alignment** – End to End Trust cannot be realized through technology alone. Technology innovation must also align with social, political, economic, and IT organizations that enable change by working across the Internet and addressing issues such as identity theft, online fraud, and child safety.

End to End Trust can only be realized through the cooperation of governments, industries, and individuals who share a vision for developing solutions that protect the safety of data and systems, mitigate the impact of cyber crime, and safeguard individual privacy. End to End Trust on the Internet requires technological innovations (such as a robust identity model) that are aligned with innovations in the social, political, and economic spheres. Microsoft is currently engaged in three key projects with government and industry partners to realize this vision:

- **Verified Identity System** – The Internet lacks a consistent and secure digital identity system that allows people to control and protect their privacy. Sometimes a digital identity requires providing full name; at other times it calls for a more specific or partial "identity claim," such as membership in an organization or proof of age or citizenship. Such digital identities should be based on a single, unified industry standard, should be flexible enough to meet the specific needs of users at any given moment, and should allow people to tailor their specific needs and work with existing and future systems.
- **Device Health** – There's a great need for a simple, consistent, and secure way to measure and independently verify the trustworthiness of devices that connect to the internet. The goal of this project is to create a standards-based solution to improve and verify computing devices that are used for high-value transactions.
- **Policy-Based Data Protection** – Sensitive data is often shared not only beyond the premises of organizations, but also on a wide variety of devices. Focused data protection mechanisms can help solve some of the problems of compromised or poorly secured data. This project focuses on creating solutions and processes that ensure persistent data protection methods that are based on policies that are applicable regardless of the location, destination, or movement of data.

Helpful Resources

www.endtoendtrust.org
Microsoft's End to End Trust website

Microsoft Approach

Microsoft is committed to realizing the vision of End to End Trust through a variety of efforts in three key areas:

Security and Privacy Fundamentals

- The Security Development Lifecycle (SDL) is an industry security assurance process that has been shown to reduce the number and severity of security vulnerabilities before software is released.
- Microsoft Privacy Guidelines for Developing Software Products and Service is a set of privacy guidelines for developing software products and services.

Technology Innovations

- Microsoft's Business Ready Security strategy is designed to help businesses securely manage risk and empower people.
- Microsoft Reputation Services allows security administrators to block inappropriate or dangerous website categories without limiting employee productivity.
- Microsoft U-Prove technology provides cryptographic techniques for strong security with additional privacy protection capabilities that include minimal disclosure.

Social, Economic, Political, and IT Alignment

- Microsoft is engaged in dialogue, collaboration, and consensus-building efforts with customers, partners, industry, and governments.

Policy Considerations

- Microsoft welcomes government support in fighting online security threats. We believe that industry's cooperation with governments and authorities is the most effective way to reduce cyber threats, and we support balanced regulation as part of that effort.
- Microsoft has joined with industry partners to encourage countries to adopt and ratify the Council of Europe Convention on Cybercrime, which requires signatories to adopt and update laws and procedures to address crime online.
- Microsoft supports government funding of basic security research to help improve the security of online systems.

Key Points

- End to End Trust is Microsoft's vision for a safer, more trusted Internet. Microsoft supports this vision through work on several key projects, including: verified identities through strong digital credentials that are based on in-person proofing; device health through measuring and verifying the health of devices that connect to the Internet and other networks; and policy-based, trusted data protection mechanisms to safeguard data wherever it is transmitted, stored, or accessed.
- End to End Trust is focused on three main areas: security and privacy fundamentals; technology innovations; and social, economic, political, and Information Technology (IT) alignment.

Collective Defense: Applying Public Health Models to the Internet

March 2011

Background

Advances in modern technology have led to remarkable global development, social change, and an evolution in the way businesses, civil society, and governments work from day to day. Today's leaders and decision-makers must respond to this new reality with new ideas and solutions—and engage as partners in the public debate on Internet safety, privacy, and accountability. The challenges are substantial and complex:

- Cyber threats have become more widespread, sophisticated, and difficult to characterize (threats have little in common in terms of origin, path, or impact), and this global issue calls for a myriad of responses and solutions.
- Botnets, the most insidious of malware, threaten infrastructure, which in turn threatens financial markets, military institutions, and national security.
- The process of transferring large amounts of data through illicit channels across geo-political boundaries has become much easier and more simplified.
- Consumers aren't security experts and never will be; voluntary behavior and market forces are preferred, but government and industry should provide a secure baseline.

One way to address cyber threats is for governments, industry, and consumers to support cyber security efforts modeled on efforts to address human illnesses. In a public health model, members must be aware of basic health risks and be educated on how to avoid them. In many schools for example, students may be required to be vaccinated before admission; warned if other students show symptoms; required to stay at home if infected; and notified and required to meet specified criteria for re-admission to school.

To improve the security of the Internet, governments and industry could similarly engage in systematic activities to improve and maintain the health of the population of devices in the computing system by promoting preventative measures, detecting infected devices, notifying affected users, enabling those users to treat devices that are infected with malware, and taking additional action to ensure that infected computers do not put other systems at risk.

Helpful Resources

www.microsoft.com/mscorp/twc/endtoendtrust/vision/internethealth.aspx
Microsoft Calls for Internet Health Model for Cyber Security Collective Defense

http://blogs.technet.com/b/microsoft_on_the_issues/archive/2010/10/05/the-need-for-global-collective-defense-on-the-internet.aspx
Collective Defense Blog

http://go.microsoft.com/?linkid=9746317
Collective Defense: Applying Public Health Models to the Internet

www.endtoendtrust.org
Microsoft's End to End Trust Vision

Microsoft Approach

Microsoft supports a collective cyber security defense similar to a public health model that limits the spread of human illness. Today, health organizations around the world identify, track, and control the spread of disease, which can include, where necessary, quarantining people to prevent the spread of infection. Microsoft believes a similar model can be used by governments and IT industry leaders to conduct a more methodical examination, prevention, and treatment of computers that may be infected with malware.

- Microsoft believes this collective approach can provide long-term solutions to improve and maintain the health of computers and other devices on the internet by detecting infected devices, notifying affected users and helping them repair devices that are infected with malware—and taking action to ensure that infected computers do not put other systems at risk. This model is just a starting point. This vision cannot become a reality without the feedback and support of government leaders, privacy advocates, Internet Service Providers (ISPs), and others in the industry.

Policy Considerations

- Citizens the world over are facing more dangers online, while businesses and governments are confronting substantial cyber security issues—all of which call for solutions made in collaboration, not isolation, with a modern frame of reference and forward-thinking ideas. Effective and far-reaching goals can be achieved if all parties agree to an open exchange of ideas and a sustained commitment to work together—to align social, economic, and political innovations and mount a collective defense against cyber threats.
- As with any international effort, every region will have differing levels of sensitivities, and we must strive for solutions that will be socially acceptable and meet with public approval—especially with respect to balancing security and privacy. Global progress on this critical issue merits a coordinated effort among industry, government, academics, and all impacted societies worldwide and an open exchange of ideas about better protecting the health of the Internet.

Key Points

- Cyber crime is a significant global problem, costing billions of dollars each year. In response, a collective defense across the entire global Internet is needed to ensure a systematic approach to dealing with these threats.
- An "Internet health model" would separate unhealthy devices from the Internet, meaning that devices that are certified as healthy can access the Internet without putting other devices at risk, and consumers can be protected with privacy in mind and without compromising freedom of expression and freedom of association.
- Any effort to promote Internet health and security can, and should be, balanced with considerations about the social, legal, and economic issues of privacy and to not adversely impact economic activity. An Internet health model will only work as a collective defense if it is accepted by society and if people are confident that their privacy is protected. To that extent, we must work to develop socially acceptable cyber health policies, laws, and international agreements.

Mandatory Encryption of Data

February 2011

Background

In recent years, a wave of highly public incidents involving the unintentional disclosure of information, known as *data breaches*, has drawn the attention of governments worldwide. In 2007, a government official lost two computer disks containing unprotected data for 25 million U.K. citizens. In 2009, a single data breach in the U.S. resulted in the compromise of over 100 million credit cards. And according to the Microsoft Security Intelligence Report (SIR), in 2010 the largest single category of data breach incidents involved stolen equipment, which account for 30.6 percent of all data breaches.

Government and industry have responded by developing measures to provide better data security, including the use of encryption technologies. Encryption is the process of making data unreadable through the use of an algorithm known as a cipher. Encryption helps protect the confidentiality of data by requiring the use of a key to decrypt the data. Data designated for encryption is typically classified by location as either *data at rest*—meaning data stored on disks, tapes, and other devices; or *data in transit*—meaning data that is being sent across private networks or the Internet. Data may also be designated by sensitivity level, for example *personally identifiable information*—information such as a name that can be used to uniquely identity someone; and *sensitive personal information*—information such as a government-issued identification number or credit card number.

In recent years, a number of governments have either enacted, or considered enacting, legislation that requires organizations to encrypt data about individuals. Proposed legislation has included protecting sensitive personal information, data in transit, or, in some cases, both data at rest and data in transit.

While encryption can, and does, play a significant role in protecting data, it is not without cost. Widespread implementation of encryption can be difficult and expensive—particularly for small businesses with limited information technology resources—and in some cases, encryption may not be the most appropriate solution to protect customer data. Additionally, many newer devices, such as smart phones, are unable to manage encrypted data.

As more governments implement data breach notification laws, which require companies and agencies to disclose to customers when there is a possible loss of their information, many organizations have responded by adopting more secure technology, including encryption. Many jurisdictions with data breach notification laws now exempt companies from disclosure requirements if the data was encrypted at the time of loss. This "encryption exemption" is a powerful motivator for companies to use encryption to protect sensitive data and avoid the serious consequences of a public data breach.

Helpful Resources

www.microsoft.com/windows/windows-7/features/bitlocker.aspx
Microsoft Windows BitLocker home page

www.microsoft.com/online/exchange-email-encryption.aspx
Microsoft Exchange Hosted Encryption home page

www.microsoft.com/sir
Microsoft Security Intelligence Report website

www.microsoft.com/security
The Microsoft security and safety website

Microsoft Approach

- Microsoft is working to make encryption technology more readily available to business, government, and consumers by promoting good security practices and providing encryption products.
- Microsoft BitLocker allows businesses and consumers to encrypt entire hard drives for Windows® 7 and Windows Vista® computers. BitLocker To Go™ allows encryption of portable storage devices such as USB flash drives.
- Microsoft Exchange Hosted Encryption provides businesses with policy-based encryption from sender to recipient with no end-user training or software.
- The Microsoft Security Intelligence Report (SIR) provides an in-depth perspective on changing Internet security threats, including the latest trends on data breaches, vulnerabilities, and malicious software that impact privacy.

Policy Considerations

- Because of the expense and complexity of deploying widespread encryption across all businesses, Microsoft believes that mandating a single standard for encrypting data is not the best way to protect data.
- Microsoft supports government measures that encourage businesses to adopt encryption through data breach notification laws that exempt encrypted data from notification requirements.
- As governments act to address issues associated with emerging technologies and online services, it is important that they do not stifle innovation and technology adoption in the process. Government and industry can work together to establish appropriate principles.

Key Points

- Microsoft strives to make encryption technology more readily available to business, government, and consumers with products like BitLocker, Drive Encryption, and Microsoft Exchange Hosted Encryption.
- Because of the expense and complexity of deploying widespread encryption across all businesses, Microsoft believes that mandating a single standard for encrypting data is not the best way to protect data.
- Microsoft supports legislation and government policies that encourage businesses to adopt encryption practices through data breach notification laws that exempt encrypted data from notification requirements.

Microsoft Security Response Center

February 2011

Background

Computer security is an ongoing, ever-changing challenge. Threats have become more complex and widespread as cyber criminals have developed sophisticated new ways to attack both large, interconnected systems and individual customers.

The Microsoft Security Response Center (MSRC) was created to help keep pace with evolving security threats and better protect customers against malicious attacks through timely security updates and authoritative security guidance. The MSRC serves as Microsoft's single point of security coordination and communications and is led by some of the world's most experienced security experts. The MSRC team works to identify, monitor, respond, and resolve security incidents and vulnerabilities, and the center is on alert seven days a week, 365 days a year.

When a security incident occurs, we combine our own efforts with those of our partners. The MSRC mobilizes internal and external security teams to provide up-to-date information, guidance, mitigation, and tools to help address the threat. Through the MSRC, Microsoft addresses security risks by:

1. Delivering security response
2. Fostering active security collaboration
3. Advancing innovation and better defenses

Microsoft Approach

The MSRC team manages more than 150,000 vulnerability reports each year, and we provide information and solutions through regular security updates, bulletins, and advisories. Our team communicates with customers through a number of channels including blogs and webcasts, and we provide regular security advisories and bulletins to help customers. When the MSRC addresses a vulnerability with an update, security experts write an accompanying bulletin, which is translated and released the second Tuesday of every month in multiple languages. Microsoft began releasing monthly security updates in 2003, and in 2005 we introduced Microsoft Security Advisories to address any other issues that might impact customer security.

The MSRC also leads the worldwide Software Security Incident Response Process (SSIRP), which is a detailed, global plan for responding to and managing critical threats as they arise. SSIRP helps us quickly and effectively investigate, analyze, and resolve security incidents and other new situations that arise when criminals deliberately exploit vulnerabilities. Other efforts include:

- **Global Conference Engagement** – The MSRC co-sponsors and participates in more than 50 security conferences each year. An open dialogue with the security research community helps us provide more timely and accurate information to better protect customers.

Helpful Resources

www.microsoft.com/security
Microsoft's online safety and security resource website with aged-based guidelines for Internet use

www.fosi.org
Family Online Safety Institute is an international non-profit organization working to develop a safer Internet

www.besmartwireless.com/
Online safety information for parents, educators, and policymakers provided by the U.S. CTIA

www.mobilebroadbandgroup.com
Coalition of mobile providers in the United Kingdom promoting social responsibility

- **Black Hat®/BlueHat Conferences** – Microsoft co-sponsors Black Hat, a premier technical security conference that includes government agencies, global corporations, and independent security researchers. We also host BlueHat conferences that allow outside security researchers to share their knowledge and expertise about the security threat environment with us.
- **Microsoft Active Protections Program (MAPP)** – The MAPP provides vulnerability information to more than 50 security software providers in advance of Microsoft's monthly security update release so customers can benefit from additional protections that third-party vendors develop.
- **Microsoft Vulnerability Research (MSVR)** – As Microsoft improves its own software security, attackers have shifted their focus to third-party applications running on the Microsoft Windows® platform. The MSVR program helps detect, report, and resolve vulnerabilities in third-party code, which benefits the entire Internet.
- **Microsoft Security Response Alliance (MSRA)** – MSRA helps independent software vendors (ISVs), governments, and infrastructure providers collaborate on security issues. The alliance offers a variety of tools to reach Microsoft security support contacts and provides a dedicated forum for anti-virus researchers to discuss options for improving the security of Microsoft products.

We advance innovation and promote better defense against cyber crime in three additional ways:

- **Industry Consortium for Advancement of Security on the Internet (ICASI™)** – Microsoft co-founded ICASI, which is a non-profit corporation of leading IT companies and a trusted forum that addresses international, multi-product security challenges.
- **The Microsoft Exploitability Index** – We launched the Microsoft Exploitability Index in 2008 to evaluate risks and help customers prioritize security updates.
- **Security Intelligence Report (SIR)** – The MSRC shares important information through a semiannual Microsoft Security Intelligence Report (SIR), which is compiled using data from hundreds of millions of computers and some of the busiest online services on the Internet.

Key Points

Microsoft collaborates with the security community and other global partners to help create a more secure computing experience and a safer, more trusted Internet environment. Microsoft takes a number of important steps to help customers stay ahead of the latest security threats:

- We work closely with security researchers, vendors, and government agencies worldwide as well as our own internal security experts. We appreciate those partnerships; they are invaluable in our efforts to better serve our customers.
- We work with a global network of security experts, researchers, law enforcement, and partners to analyze and respond to new threats, and we closely monitor security news lists and public forums.
- Microsoft Security Response Center (MSRC) researchers conduct detailed technical investigations of software security issues, and we share our findings with security engineers and software developers around the world to help mitigate current and future attacks. Sharing information in this way helps reduce the number and severity of vulnerabilities in future products—and supports the Microsoft Security Development Lifecycle.

Microsoft® Security Intelligence Report (SIR)

November 2010

Background

The Internet has become an integral part of day-to-day life. As the number of online users increases, so too have concerns about safety online. Dramatic increases in Internet traffic have produced similar increases in online-related crime, and online security is a growing concern for governments, organizations, and individuals worldwide.

Online threats have evolved from petty crimes by attention-seeking hackers to multi-front attacks by more sophisticated criminal organizations. Cyber criminals exploit users through email, web browsers, social media, online games, and false security software. Compromised computers can be used to breach complex security systems, target financial institutions and political organizations, or rob consumers of money and a sense of security.

As a partner in the global response to online crime, Microsoft provides resources and expertise to help determine the latest threats and promote a culture of online safety. Microsoft's biannual Security Intelligence Report (SIR), provides a comprehensive, up-to-date, and geographically relevant analysis of the cyber threat landscape.

Microsoft appreciates the scope and changing complexities of online security—as well as the tremendous value of collaborative efforts to provide the most up-to-date information, support, and guidance. We continue to promote the global imperative of sharing knowledge with industry leaders, governments, and security organizations. By further developing and supporting global partnerships, we can better assist policymakers, organizations, and consumers who must make prompt, relevant decisions about their privacy and safety online.

Microsoft Approach

The proactive work of the Trustworthy Computing (TwC) group focuses on three areas that directly benefit the security of Microsoft's customers and the entire Internet: Security Science, the Security Development Lifecycle, and Critical Infrastructure Protection.

- **Security Science** – driving security innovations for customers and Microsoft. Building on a body of research about ways that systems are attacked and ways to prevent or mitigate attacks, Security Science incubates and develops tools and techniques that make it more difficult to successfully attack software. Security Science continually monitors threat trends and activities in the threat landscape and uses that information to improve our tools and processes. We continually look for software vulnerabilities and develop and exploit mitigation tools and techniques that developers can use for improved security and better overall protection.
- **Security Development Lifecycle (SDL)** – improving the fundamentals by releasing software that is more secure. The SDL is an industry security assurance process that has been shown to reduce the number and severity of security vulnerabilities before software is released. Microsoft freely shares the SDL with the software industry and customers' development organizations so it can be used to create more secure software.
- **Critical Infrastructure Protection** – improving cyber security by aligning technology and policy worldwide. With technology becoming more important to the lives of Internet users every day, Trustworthy Computing engages with governments around the world to help them protect critical infrastructures and the safety of their citizens online. TwC is committed to sharing our research and innovations to help establish policies that make meaningful improvements to cyber security globally.

Policy Considerations

- Microsoft welcomes the support of governments in fighting online security threats. We believe that industry cooperation with authorities is the most effective means of reducing overall cyber threats, and we support balanced regulation as part of that effort. We believe that less onerous restrictions on industry allow for greater innovation and flexibility in developing and implementing responses to cyber crime.
- Microsoft has joined with industry partners to encourage countries to adopt and ratify the Council of Europe Convention on Cybercrime, which requires signatories to adopt and update laws and procedures to address crime in the online environment.
- Microsoft supports the funding of basic security research by governments in order to help improve the security of online systems.

Helpful Resources

www.microsoft.com/msrc
Microsoft Security Response Center (MSRC) website

www.microsoft.com/sir
Microsoft Security Intelligence Report website

www.microsoft.com/security_essentials
Microsoft Security Essentials

www.microsoft.com/sdl
Microsoft Security Development Lifecycle (SDL) website

www.microsoft.com/mmpc
Microsoft Malware Protection Center (MMPC) website

Key Points

The SIR details trends in data breaches, vulnerabilities, and the impact of malicious software. The report also offers guidance about protecting networks, systems and users, and it provides information about mitigating the impact of Trojans, spam, and botnets. Findings include:

- Continued downward trend in reported vulnerabilities and security breaches of Personal Identifiable Information, or PII. Losses dropped 46 percent in the first half of 2010 compared with the same period in 2009.
- Strong evidence of greater integration between malicious threats and botnets that replicate online crime by surreptitiously compromising computers and enabling them to transmit information, including spam and viruses, to other computers over the Internet.

The Microsoft Security Development Lifecycle (SDL)

November 2010

Background

Today's cyber security threats are complex, sophisticated, and ever-changing, and as such they require an ongoing, multi-faceted, and unified response to develop the most effective solutions for a safer computing experience and a more secure Internet environment.

The Microsoft Security Development Lifecycle (SDL) is Microsoft's security assurance process for software development that offers a full-system response to evolving security threats and increasingly sophisticated cyber crime. The SDL combines a holistic and practical approach to introduce security and privacy throughout all phases of the development process, with the goal of optimizing software security and protecting and supporting customers worldwide.

Since Microsoft's adoption of SDL in 2004, we have seen significantly reduced vulnerabilities in products such as Windows Vista®, Microsoft Office, and Microsoft SQL Server™. We have also learned that security activities that are executed in chronological order, as part of a repeatable process, result in greater security gains and cost savings, and create a better, more secure Internet environment for everyone. With that in mind, Microsoft makes SDL resources including tools, education, and processes available to software developers, partners, and others in the global IT industry.

Microsoft Approach

Microsoft developed the SDL process in 2004 as part of a defense-in-depth approach to reduce the number of vulnerabilities in software and provide customers with high-quality, meticulously engineered, and rigorously tested software that better defends against malicious attacks.

The SDL encompasses a systematic series of mandated security and privacy focused activities and deliverables, which include engineer training and continuing education, software design, code reviews, and security and privacy testing.

While it's impossible to completely prevent all vulnerabilities during software development, we can build protections in place when vulnerabilities do surface. Software development is an evolving process – each time a vulnerability is identified, the SDL process allows us to take steps to understand what happened in the software development process and incorporate that knowledge into the next version of the SDL.

Helpful Resources

www.microsoft.com/sdl
A paper on "The Trustworthy Computing Security Development Lifecycle"

www.microsoft.com/twc
Microsoft's Trustworthy Computing website

The SDL is updated regularly to reflect the knowledge and proven practices across all phases of the software development lifecycle. We've seen measurable improvements in the security and privacy of Microsoft's software since the SDL process was implemented:

- In the first year of its release, Windows Vista contained 66 vulnerabilities compared to 119 vulnerabilities found in Window XP – a resulting 45 percent decrease. (Source: Windows Vista Once Year Vulnerability report.)
- One year after release, Microsoft Internet Explorer® 7 contained 17 vulnerabilities compared to Microsoft Internet Explorer 6, which contained 26 vulnerabilities. Overall, there was a 35 percent decrease in vulnerabilities and a 65 percent decrease in high-severity vulnerabilities. (Source: Internet Explorer Vulnerability Analysis report.)

While determined criminals continue to broaden their scope of attack, we remain focused on reducing the number and severity of vulnerabilities in our products and ensuring that our customers have a trustworthy computing experience. We are committed to building secure, reliable software, and we believe that the SDL is an industry-leading assurance process for doing so.

Key Points

The Microsoft SDL is a cultural, as well as technological, transformation that guides every part of our development cycle. The SDL process:

- Builds security into every phase of software development and provides "defense-in-depth" guidance and protection;
- Is a "bottom up" as well as "top down" creative process, with product security teams in Office, Windows®, SQL Server, and other departments working on security innovations that are integrated with the companywide SDL policy and shared with external audiences;
- Is a continuously evolving and improving system of requirements and technologies that is regularly updated in six-month cycles to take advantage of newly developed techniques in security science and is used to stay ahead of emerging threats;
- Is not specific to Microsoft or the Windows platform. It can be applied to different operating systems, platforms, development methodologies, and to projects of any size.

Microsoft is committed to protecting customers and creating a more trusted computing experience and a more secure Internet environment. One way to reach this goal is by sharing security expertise, guidance, technology, and processes. To that end, we provide SDL resources, including tools, education, and processes to partners and organizations that focus on software development, security, research, and IT systems worldwide.

Privacy

February 2011

Background

The digital economy has changed the world in profound and exciting ways. At the same time, concerns about the collection and use of personal information, widely publicized data breaches, and online fraud all threaten to erode public confidence in digital commerce and the computing ecosystem.

Consumers have high expectations about how companies collect, use, and store their information. The public's trust depends on people knowing that their privacy will be protected and that their personal information will be used appropriately. If companies fail to meet these standards, consumers will be less inclined to use online technologies, and both industry and individuals will suffer from a lack of trust.

Microsoft and all companies that operate online must adopt strong privacy practices that protect customer trust.

Microsoft Approach

- **Privacy Fundamentals** – People and processes are at the core of our efforts to give individuals greater control over their personal information and to help organizations manage data more responsibly and with greater accountability. Hundreds of people across Microsoft work to ensure that privacy policies, procedures, and technologies are applied across the company's products, services, processes, and systems. Our privacy principles and corporate Privacy Statement, our use and management of customer and partner data, and our rigorous technical development standards help ensure that privacy and data protections are systematically incorporated into the development of Microsoft's products and services.
- **User Empowerment, Protection, and Control** – Microsoft provides strong data protection tools and clearly worded privacy policies with all of our offerings, which include more than 200 online services and Web portals. Our software products are designed to help individuals block unwanted communications, protect themselves from potentially dangerous online content, and control the details of their online activities. We also offer many free educational resources to help people manage their privacy and information online.

Helpful Resources

www.microsoft.com/privacy
An overview of Microsoft privacy policies and initiatives

www.microsoft.com/privacy/principles
Microsoft's Privacy Principles

www.microsoft.com/privacy/principles.aspx
Privacy Guidelines for Developing Software Products and Services

www.microsoft.com/privacy/cloudcomputing.aspx
Privacy and Cloud Computing at Microsoft

- **Data Governance and Compliance** – To help organizations safeguard confidential data, Microsoft offers a data governance framework and shares best practices to help address privacy, confidentiality, and related regulatory compliance requirements. We also help organizations fulfill their privacy, data protection, and compliance responsibilities for both locally-based and Internet-based storage, management, use, and protection of data.
- **Policy Leadership and Collaboration** – Microsoft works with governments, businesses, and other industry leaders to advise on legislative proposals, align laws across jurisdictions, develop responsible business practices, and strengthen self-regulatory mechanisms that support greater protections for individuals and their personal information. Our public policy efforts include advocating for new and updated regulatory approaches to promote a safer, more open cloud computing environment. We also work with multilateral organizations, law enforcement agencies, and consumer and advocacy organizations worldwide to combat online fraud, spam, spyware, and other threats.

Policy Considerations

- Microsoft supports privacy legislation initiatives that facilitate the free flow of information, build trust, and encourage innovation. Because many data exchanges are global, we favor greater alignment of privacy regulations, policies, and standards on a global scale.
- As governments act to address issues associated with emerging technologies and online services, they should not stifle innovation and technology adoption in the process. Government and industry can work together to establish appropriate and balanced principles that can be standardized and applied globally.
- Microsoft welcomes the support of governments in fighting online crime. In general, we believe that cyber threats are most effectively reduced when industry cooperates with authorities, and we support balanced regulation as part of that effort. We also favor regulatory approaches that encourage flexible and innovative industry responses to rapidly evolving threats to privacy.

Key Points

- Microsoft's long-standing commitment to privacy includes tools, technologies, people, processes, and procedures for embedding privacy protections in our products and services—from development through deployment and operation.
- Microsoft employs more than 40 people who work full-time on privacy, and another 400+ employees worldwide focus on privacy as part of their jobs.
- Microsoft supports privacy legislation initiatives that facilitate the free flow of information, build trust, and encourage innovation. Because data is increasingly flowing across geopolitical borders, we favor greater standardization and better alignment of privacy regulations, policies, and standards worldwide.

Privacy Accountability

March 2011

Background

Accountability is a long-established principle of privacy and data protection. The concept of data protection accountability was first established by the Organisation for Economic Co-operation and Development (OECD) in the early 1980s. The intent of accountability can be found in the law of the European Union and EU member states, and is outlined more explicitly in the Canadian Privacy Law (PIPEDA) and the APEC Privacy Framework.

While the concept of accountability for data protection and privacy is not new, much has changed in the realm of information. These changes are the result of trends that include innovations in technology; expansive data collection, analysis and processing; greater access and flow of data worldwide; and powerful analytics – all available in an unprecedented array of products and services. These trends underscore the importance of accountability because more data about more people is even more accessible than ever before. Collection and use of personal information has become a more common practice, and that information comes from many sources and can be collected in ways that are less transparent. This makes it challenging for individuals to understand and control how their information is collected and used.

Countries have responded in a variety of ways – with explicit data protection laws, through regional or self-regulatory frameworks, or by promoting commonly accepted principles. Yet the individual consumer still bears much of the burden for ensuring that their personal information is stored and used appropriately.

Under the principle of accountability, an organization is responsible for understanding and mitigating the risks to individuals that come with the processing of their information.

Elements of an accountability approach for organizations include:

- Demonstrating a commitment to accountability and adopting internal policies that are consistent with external criteria;
- Creating, adopting, or enacting privacy policies that include the use of tools, training, and education;
- Implementing systems for internal, ongoing oversight, assurance reviews, and external verification;
- Improving transparency and mechanisms for individual participation;
- Establishing a means for remediation.

Furthermore, an organization must be responsible for ensuring that its internal processes safeguard customers' data. Accountability requires more diligence and vigilance from an organization than basic compliance with the law.

Helpful Resources

www.microsoft.com/privacy
An overview of Microsoft privacy policies and initiatives

www.microsoft.com/privacy/principles
Microsoft's Privacy Principles

http://www.microsoft.com/privacy/principles.aspx
Data Protection Accountability: The Essential Elements, Centre for Information Policy Leadership

Microsoft's View

- A key Microsoft privacy principle is that of accountability in handling our customers' personal information within the company and with our vendors and partners.
- Each Microsoft business unit is responsible for developing procedures to strengthen and support accountability and for assigning specific staff members the day-to-day responsibilities of privacy protection, enforcement, and monitoring.
- Microsoft believes that policymakers and other relevant stakeholders should carefully consider how the accountability model might work within legal regimes, how organizations can do more to advance accountability, and what role third-party accountability agents and other validation programs might play in this evolving paradigm.

Policy Considerations

- Accountability has long been a principle of Fair Information Practices, the Organisation for Economic Co-operation and Development (OECD) privacy principals, and the APEC Privacy Framework. Accountability involves setting privacy protection goals for companies based on established data protection regulatory regimes rather than seeking to replace existing data protection regulations.
- Any government approach to addressing issues of emerging technologies and online services should likewise protect the principles of innovation and ensure the continued adoption of new technologies. Government and industry can work together to establish appropriate principles and strike the right balance between regulation and innovation.

Key Points

- Under the principles of accountability, an organization is responsible for understanding the risks to individuals that are inherent in processing their personal or sensitive data; for creating policies, tools, and processes to mitigate those risks; and for ensuring that internal privacy controls safeguard individual customer data.
- One of the key Microsoft privacy principles is accountability for the way that personal information is controlled by Microsoft or its external vendors and partners. Each Microsoft business unit is responsible for developing procedures to uphold the company's accountability commitment.
- Microsoft believes that policymakers and other key stakeholders should carefully consider how the principle of accountability might work throughout legal jurisdictions, how organizations can do more to advance accountability, and what role third-party accountability agents and other validation programs might play in this evolving paradigm.

Enabling Privacy with Data Governance

March 2011

Background

Personal information shared over the Internet fuels a wealth of business activities. However, as organizations collect growing volumes of personal data and seek to use it in more diverse ways, they also must contend with greater risks of data breaches, theft, and misuse of personal data and potential violations of an organization's own privacy policy or regulations. These factors, along with widely publicized data breaches and growing public concerns about identity theft and online tracking, threaten to limit the growth of online commerce and services. Organizations that fail to manage and protect personal information face considerable risks—including damaged reputation, penalties and sanctions, lost market share, and needless expense.

Through data governance, policies, and processes are developed to ensure that information and data assets are used and managed to their fullest potential. Data governance includes managing data-related risks, strengthening security and privacy protections, and ensuring compliance.

Effective data governance that is based on a sound framework can help organizations protect and manage personal information, mitigate risk, achieve compliance, and promote trust and accountability.

Microsoft Approach

Microsoft has developed a privacy, confidentiality, and compliance framework for data governance that can be adopted and implemented by organizations of all sizes. A series of whitepapers and webcasts describing this framework, along with support resources, are available as free online resources.

Key elements of the framework include:

- **People** – A virtual organization that can set the appropriate goals and objectives as well as define and implement the policies, processes, and control objectives.
- **Process** – A process model that supports an organization's efforts to better understand privacy, confidentiality, and compliance needs and obligations, and outlines the governance mechanisms necessary to ensure these obligations are met.
- **Technology** – Technology tools and techniques that allow an organization to identify and address security, privacy, and compliance-related risks by analyzing key components of information technology and communications systems.
- **The Information Lifecycle** – Selecting technical controls and activities to effectively protect confidential data requires an understanding of how information flows throughout an organization over time and how information is accessed and processed at different stages by multiple applications and people and for various purposes. The information lifecycle better facilitates an understanding of these requirements.

Helpful Resources

www.microsoft.com/datagovernance
Microsoft's Data Governance website

- **Technology domains** – Data governance includes four technology domains:
  - » **Secure Infrastructure** – Since 2003, Microsoft has built security into its products from the ground up with the Security Development Lifecycle (SDL), which is a rigorous design process that helps remove vulnerabilities and minimize malicious attacks.
  - » **Identity and Access Control –** Microsoft offers authentication and authorization technologies, including Active Directory and Forefront® Identity Manager, that help prevent unauthorized access to information while facilitating its availability to legitimate users. Forefront® Identity Manager.
  - » **Information Protection** – Microsoft products include data encryption and rights management technologies that help safeguard information against data breaches resulting from loss or theft, including BitLocker Drive Encryption and Active Directory Rights Management Services.
  - » **Auditing and Reporting** – Microsoft System Center provides products that can be used to verify that systems and controls are operating effectively and to identify suspicious activity.

Policy Considerations

- By adopting data governance policies and processes, governments can demonstrate a commitment to privacy protection and an understanding of implementation that can form the basis of future policy positions and legislation.
- Governments are uniquely positioned to promote data governance through academic programs, public-private partnerships, government-sponsored publications, and conferences. The insights that governments gain by adopting data governance, when shared freely, are valuable tools for promoting data governance.

Key Points

- Data governance is the application of policies and processes designed to ensure that information and data assets are used and managed to their full potential. Proper governance includes managing risks related to data, strengthening security and privacy protections, and ensuring compliance.
- Microsoft has developed a privacy, confidentiality, and compliance framework for data governance that can be adopted and implemented by organizations of all sizes and types. Key elements of this framework include:
  - » People – A virtual organization that can set the appropriate goals and objectives as well as define and implement a means of achieving them.
  - » Process – A process model that will support the organization's efforts for privacy, confidentiality, and compliance.
  - » Technology – Technology tools and techniques that allow organizations to identify and address security, privacy, and compliance-related risks.
- Governments are uniquely qualified to advance the adoption and implementation of data governance within organizations—and ultimately enhance the privacy protections of their citizens—through thoughtful, effective policy positions and legislation.

International Privacy Standards

February 2011

Background

The Internet and cloud computing are forging a new world of information sharing online and erasing geographic boundaries for the flow of information. This international flow of information benefits the global economy in many ways: it delivers new efficiencies, opens up new markets, and creates tremendous opportunities. The Internet makes it possible for a business in one country to run a website or store data in a second country, and conduct transactions with customers the world over.

Yet when disputes arise over data, it's not always clear which laws, regulations, and data protection principles apply. While information sharing technology has undergone tremendous change, today's regulatory models are based on a way of life that existed before today's digital globalization. In the member states of the European Union, the European Commission's Directive on Data Protection places controls on the use and transmission of personal data to other nations. In the United States, statutes and regulations for data exchanges vary not only from state to state, but also by age and industry. In the United States, different privacy laws apply to children, healthcare, and finance. For companies that conduct international business, complex compliance requirements add to the cost of doing business.

Industry needs to work with government to develop more consistent and constructive privacy protection frameworks that streamline an increasingly complex set of international, regional, and local laws governing privacy and data protection. In recognition of this need, the 32nd International Conference of Data Protection and Privacy Commissioners passed a resolution in 2010 that calls for the organization of an intergovernmental conference with a goal of developing a binding international instrument on personal data protection and privacy.

Microsoft Approach

- Microsoft's longstanding commitment to privacy includes principles, policies, and procedures for building privacy protections into our products and services—from development through deployment and operation.
- Microsoft's privacy standards govern the development and deployment of Microsoft consumer products and services. These standards (a version of which has been made public) include detailed guidance on creating customer notification and consent procedures, providing sufficient data security features, maintaining data integrity, and providing user access and necessary controls.
- Microsoft shares its views about many of the privacy-related legislative proposals that are taking shape around the world. Our efforts include providing information and feedback to the United States Federal Trade Commission on its Self-Regulatory Principles for Behavioral Advertising; participating in the European Commission's consultation process for the European Union Data Protection Directive; and supporting the development of the Asia-Pacific Economic Cooperation Privacy Framework.

Policy Considerations

- Microsoft supports efforts to develop globally consistent policy frameworks that recognize the worldwide nature of data exchanges and provide strong privacy protections. Governments can help develop clear rules and processes to resolve conflicting privacy obligations.
- International privacy standards should be flexible and technology neutral, and they should be applied across sectors.
- Microsoft believes the way data is used, rather than how it is collected, is a better basis for defining data protection and privacy obligations related to that data. Microsoft supports an approach that emphasizes "use and obligations" rather than relying on "notice and consent."
- In order to optimize the efficiency of online services and deliver on the promise of performance and reliability that customers expect, cloud providers should be able to operate data centers in multiple locations worldwide and transfer data freely among them.

Helpful Resources

www.microsoft.com/privacy
Microsoft privacy website, with links to white papers and backgrounders

www.microsoft.com/privacy/cloudcomputing.aspx
Microsoft's Privacy in the Cloud website

www.microsoft.com/privacy/bydesign.aspx
Privacy by design at Microsoft

Key Points

- Cloud computing and international commerce are limited by conflicting international laws and regulations governing the privacy of data that's sent across international borders.
- Microsoft supports efforts to develop globally consistent policy frameworks that recognize the worldwide nature of data exchanges and provide strong privacy protections. Governments need to help develop clear rules and processes to resolve conflicting privacy obligations.
- International privacy standards should be flexible, applied across sectors, and technology neutral. Strong collaborations among industry, government, and advocates are needed to achieve the right balance.

Location-Based Services and Privacy

January 2011

Background

Location-based services (LBS) provide information and offer services to customers using geographic location data. Geolocation data is gathered in a number of ways, including through built-in Global Positioning System (GPS) devices, IP address, or Wi-Fi network mapping. Location-based services offer a number of useful applications, including real-time navigation software, location-based social networking services that allow customers to voluntarily "check in" their locations, and geographically targeted search engine results. The majority of applications for LBS are used in mobile services, but there are also important LBS uses for desktop and laptop computers, including mapping and search engine results.

A 2010 survey conducted for Microsoft of the United Kingdom, Germany, Japan, the United States, and Canada found that 94 percent of consumers who had used location-based services considered them valuable, but the same survey found that 52 percent were concerned about potential loss of privacy.

Among the privacy concerns related to location-based services:

- **Notice** – Customers want to receive adequate notice that by using an application they are allowing the collection and use of geolocation data.
- **Control** – Customers want to have access to, and be aware of, controls to limit the collection and use of geolocation data.
- **Retention** – Customers want to be informed about policies governing the retention of geolocation data.
- **Reuse** – Customers want to be aware of, and given choices over, how geolocation data is used and how it might be combined with other data.
- **Third-parties** – Customers want to be aware of, and have control over, the sharing of geolocation data with third-party applications.
- **Court orders** – Customers want to be aware of how geolocation data might be requested by court order.

Helpful Resources

www.microsoft.com/privacy
An Overview of Microsoft Privacy Policies and Initiatives

www.microsoft.com/privacy/principles
Microsoft's Privacy Principles

www.microsoft.com/privacy/principles.aspx
Windows Phone: Location and Privacy Questions and Answers

www.microsoft.com/maps/streetside.aspx
Bing Maps Privacy Questions and Answers

www.microsoft.com/privacy/dpd
Microsoft Data Privacy Day Survey on Location-Based Services

Microsoft Approach

- Microsoft is involved in multiple aspects of providing LBS, including as both a provider of applications, as well as an operating system platform for third-party applications. When Microsoft acts as a platform for third-party applications that use LBS, customers are notified when programs access information about location.
- Microsoft applications that use location-based services at Microsoft are governed by the Microsoft Privacy Principles, which address Accountability, Notice, Collection, Choice and Consent, Use and Retention, Disclosure of Onward Transfer, Quality Assurance, Access, Enhanced Security, and Monitoring and Enforcement.
- Microsoft applications that use location-based products and services undergo a privacy review designed to identify privacy issues and help product teams follow Microsoft privacy policies and standards. Once a product or service is released, the appropriate business group within Microsoft ensures compliance with corporate privacy requirements.
- Windows Phone – Before any Windows Phone application can gain access to information regarding a customer's location, the customer must allow the application to access the device's location. Applications that use location are required to provide the ability to turn off that application's access to an individual's location. Customers can always turn off access to location for all applications by turning off location services.

Policy Considerations

- Microsoft has a long-standing commitment to baseline privacy legislation initiatives that facilitate the free flow of information, build trust, and encourage innovation.
- As governments act to address issues associated with emerging technologies and online services, it is important that they not stifle innovation and technology adoption in the process. Government and industry can work together to establish appropriate principles.

Key Points

- Location-Based Services (LBS) offer many useful applications, such as real-time maps and the ability to locate local business, but customers will not realize the promise of LBS without the adoption of proper privacy safeguards.
- Microsoft's privacy standards govern the development and deployment of location-based services. These standards include customer notification and consent procedures, and providing sufficient data security features and adequate privacy controls.
- Microsoft believes that the information and communications technology industry should work with civil society, governments, and others to create appropriate guidance for protecting the privacy of personal location data.

Privacy in Online Advertising

March 2011

Background

Today nearly 1.6 billion people connect to the Internet for information, entertainment, social networking, and business—more than four times the number of people online just 10 years ago—and where consumers go, advertisers follow. The advertising industry's shift to virtual markets in the online world has fueled enormous growth: from the depth and breadth of Internet content to local, regional, and international economies.

Online advertising makes it possible for people to have free (or low-cost) access to an incredible amount of Web content and services, which range from news, research, and entertainment to email, instant messaging, and social networking.

A 2008 study by the European Interactive Advertising Association found that 80 percent of European Internet users have purchased products or services online—a pattern that has doubled since 2004. When advertising is based on information about individual interests and preferences that are collected from consumers as they use the Internet, both business and consumers benefit.

Consumer advocates and government organizations such as the U.S. Federal Trade Commission (FTC) and the European Union (EU) are mindful of both the benefits and drawbacks of online advertising, and they have called for better privacy and protection in this area. The EU's Commissioner for Consumer Protection recently called on the industry to "ensure that important issues of personal privacy—data collection and profiling practices—do not damage trust in the digital space." Similarly, the FTC's Self-Regulatory Principles for Online Behavioral Advertising outline the need for greater transparency, more consumer control over privacy, and improved measures to protect consumer information.

Microsoft Approach

Microsoft's approach to online advertising combines strong internal business practices with support for uniform standards of industry self-regulation and baseline national or regional legislation to strengthen privacy and data protection. We also support industry efforts to promote transparency and accountability in online advertising. Additional efforts include:

- **The Microsoft Online Privacy Statement** – provides consumers with important information about our privacy practices in a concise, one-page, up-front summary with links to more in-depth information about our data collection and use practices. Customers can make their opt-out choices both persistent and "roamable" (their choices will apply on any computer they log onto with their Windows Live™ ID).

Helpful Resources

www.microsoft.com/privacy
An overview of Microsoft privacy policies and initiatives

www.microsoft.com/privacy/principles.aspxs
Microsoft's Privacy Principles

http://go.microsoft.com/?linkid=9702232
Privacy Protections in Microsoft's Ad Serving System and the Process of "De-identification"

- **The Self-Regulatory Program for Online Behavioral Advertising** – includes an "About our ads" link on the bottom of pages that include ads or collect information for use in behavioral advertising.
- **Microsoft Internet Explorer® 9** – offers groundbreaking "do not track" functionality, known as "Tracking Protection," which gives consumers unprecedented control over the collection and use of their information online by allowing them to filter content and decide which sites can collect their data.

Policy Considerations

- Consumers want to be informed and notified about company privacy policies and the information they collect and use for online behavioral advertising. As information used in delivering ads becomes more personal and sensitive, organizations should provide additional privacy safeguards—such as allowing opting-out of behavioral ads, and requiring opt-in consent before collecting and using consumer information for advertising.
- Governments should strive to address issues associated with emerging technologies and online services with an approach that protects consumers while continuing to encourage innovation and the adoption of new technology. Government and industry can work together to establish appropriate principles.
- Microsoft supports harmonized privacy legislation in the United States across all industries and in addition to sound business practices and principled self-regulation.

Key Points

- Consumer trust is essential to the success of online business – especially when it comes to advertising online. Striking the right balance of interests in business, economics, and individual privacy benefits everyone in the long-run: from the online consumer who has more knowledge, choice, and control; to the advertisers who have more information about their markets; to the online content providers who can offer much greater value and variety because of advertising.
- Microsoft's online advertising approach is based on our overall commitment to strengthening consumer privacy across all aspects of the Web. We provide privacy information notices through a variety of channels and methods, and we support greater transparency by providing specific, accurate, and complete information disclosure statements that are easily understood and clearly presented.
- Microsoft's approach to online advertising combines strong internal business practices with support for uniform standards of industry self-regulation and national legislation to strengthen privacy and data protection.

Privacy by Design at Microsoft

November 2010

Background

"Privacy by Design" has become a popular term in the privacy community, but it means different things to different people. At Microsoft, Privacy by Design describes not only how we build products, but how we operate our services and conduct business as an accountable technology leader. We believe that Microsoft, and all companies operating online, should adopt privacy practices that build trust with the customers that use their products and services. Microsoft addresses Privacy by Design with principles, policies, and procedures to establish privacy-specific design objectives for our software products and online services at the outset of development. We continue to address privacy and data security considerations throughout the product lifecycle, and we use internal processes to track compliance.

Microsoft has a longstanding commitment to privacy. Microsoft was one of the first companies to appoint a chief privacy officer, an action we took more than a decade ago. Microsoft currently employs more than 40 people who focus on privacy full-time, and another 400 across the company and around the world who support privacy as part of their jobs. Microsoft's commitment to privacy begins with the Microsoft Privacy Principles, which address Accountability, Notice, Collection, Choice and Consent, Use and Retention, Disclosure of Onward Transfer, Quality Assurance, Access, Enhanced Security, and Monitoring and Enforcement.

In addition, Microsoft Research employs more than 800 researchers, including some of the world's finest computer scientists, sociologists, psychologists, mathematicians, physicists, and engineers, working across more than 55 areas of research, including privacy related projects such as database privacy, social media usage, cryptography tools for cloud computing, and community information management.

Examples of Microsoft Approach

- Windows Live Messenger's privacy settings allow people to specify who can view their information and activities.
- Microsoft Internet Explorer® 8's InPrivate browsing and filtering features provide people with privacy options to minimize third-party tracking of their online activity.
- Kinect™ for Xbox360®, a hardware add-on for the popular game console that uses facial and body recognition technology to identify players and control game play, was designed in cooperation with privacy experts throughout the company. Each feature was evaluated and embedded with privacy controls, where appropriate.

Helpful Resources

www.microsoft.com/privacy
An overview of Microsoft privacy policies and initiatives

go.microsoft.com/?linkid=9746120
Privacy Guidelines for Developing Software Products and Services

http://go.microsoft.com/?linkid=9746120
Privacy and Cloud Computing at Microsoft

www.microsoft.com/privacy/principles.aspx
Microsoft's Privacy Principles

- Microsoft's U-Prove technology enables online service providers to authenticate user identities to complete transactions while allowing those involved to disclose as little personal information as possible.
- Microsoft BitLocker® enables the encryption of the entire contents of hard drives and portable storage drives, protecting privacy.

Policy Considerations

- Microsoft encourages other companies to adopt the concepts of Privacy by Design. We do so by openly sharing our guidelines and processes to build privacy into products and services through design, development, and deployment.
- Privacy by Design principles are fundamental and can be supplemented by consumer education, self-regulation, and carefully crafted legislation. Such legislation should provide incentives to adopt privacy by design processes that are technology neutral and do not serve to stifle product development and innovation.
- Microsoft supports baseline privacy legislation initiatives that facilitate the free flow of information, build trust, and encourage innovation. As data flows are global, we strive to create greater harmonization of privacy regulations, policies, and standards on a worldwide basis.

Key Points

- Microsoft's long-standing commitment to privacy includes tools, technologies, people, processes, and procedures for embedding privacy protections in our products and services—from development through deployment and operation.
- Microsoft employs more than 40 people who work full-time on privacy, and another 400+ employees worldwide focus on privacy as part of their jobs.
- Microsoft supports privacy legislation initiatives that facilitate the free flow of information, build trust, and encourage innovation. Because data is increasingly flowing across geopolitical borders, we favor greater standardization and better alignment of privacy regulations, policies, and standards worldwide.

Privacy in the Cloud

February 2011

Background

A new generation of technology is transforming the world of computing. Advances in Internet-based data storage, processing, and services—collectively known as "cloud computing"—have emerged to complement the traditional model of running software and storing data on premises or on personal devices. While computing services have been offered over the Internet for years, some aspects of cloud computing are new, such as data centers in multiple locations, and shared storage and processing of personal data.

Cloud computing raises important policy considerations about how organizations handle information and interact with cloud service providers. In the traditional information technology model, an organization is accountable for all aspects of data protection, from how it uses personal information to how it stores and protects data stored on its own computers. Cloud computing differs because information can flow offsite to data centers owned and managed by cloud providers. Defining the allocation of responsibilities and obligations for security and privacy between cloud customers and cloud providers—and creating sufficient transparency about the allocation—is a new challenge.

Another important policy consideration is the regulation of cross-border data flows. As cloud computing evolves, traditional geographical limits on the movement of data are changing; for example, data might be created in France using software hosted in Ireland, stored in the United States, and accessed in Singapore. In order to realize the efficiency of cloud services and deliver the performance and reliability that customers expect, cloud providers must be able to operate data centers in multiple locations and transfer data freely among them. Unhindered data flows allow cloud providers to provide efficient service and deliver the performance and reliability that customers now expect. The benefits of cloud computing are limited by regulations that restrict cross-border data transfers, or create uncertainty, by failing to clearly articulate the rules that apply to such transfers.

Cloud computing offers both organizations and individuals the benefits of enhanced choice, flexibility, and cost savings. Regulators and lawmakers around the world can help fulfill the potential of cloud computing by resolving legal, jurisdictional, and regulatory uncertainties.

Helpful Resources

www.microsoft.com/privacy
Microsoft privacy information website

www.microsoft.com/privacy/cloudcomputing.aspx
Microsoft Privacy in the Cloud website, with white papers and other privacy resources

Microsoft Approach

- Microsoft understands that strong privacy protections are essential to building trust in cloud computing and allowing this emerging service to reach its full potential. We invest in building secure and privacy-sensitive systems and data centers that help protect individual privacy, and our business practices adhere to clear, responsible policies in this area—from software development through service delivery, operations, and support.
- Microsoft has been addressing privacy issues associated with online services since the launch of our MSN® network in 1994. We presently manage a cloud-based infrastructure and platform that supports more than 200 online services and websites. We operate one of the largest online email systems, Hotmail®, with more than 350 million active accounts, and Xbox LIVE® allows more than 25 million gamers to compete against one another online.
- Microsoft's long-standing commitment to privacy includes principles, policies, and procedures for embedding privacy protections into our products and services from development through deployment and operation. Microsoft employs more than 40 people who focus on privacy full-time, and another 400 Microsoft employees worldwide support privacy as part of their jobs. We recognize that cloud services pose unique security and privacy challenges, and we believe that our policies and practices provide a solid foundation for addressing customer concerns and building greater trust in cloud computing.

Policy Considerations

- To optimize the efficiency of cloud services and deliver the performance and reliability that consumers have come to expect, cloud providers must be able to operate data centers in multiple locations and transfer data freely among them. Unhindered data flows allow cloud providers to deliver optimal efficiency, performance, and reliability to customers. Regulations that restrict cross-border data transfers, or create uncertainty by failing to clearly articulate the rules that apply to such transfers, will limit the benefits and potential use and growth of cloud computing.
- Cloud providers are limited by the conflicting legal obligations and competing claims of jurisdiction that different governments exercise over their data. Divergent rules on privacy, data retention, law enforcement access, and other issues can lead to ambiguity and significant legal challenges.
- Cloud providers must ensure that they put security, privacy, and reliability at the center of the design of their cloud service offerings. For our part, Microsoft uses the Security Development Lifecycle to ensure that both security and privacy are built into the development of our cloud offerings.

Key Points

- Cloud computing offers organizations and individuals enhanced choice, flexibility, and cost savings. Regulators and lawmakers around the world can help fulfill the potential of cloud computing by resolving legal, jurisdictional, and public policy uncertainties that limit the growth of cloud services.
- Cloud computing raises important policy considerations about the ways that organizations manage information and interact with cloud providers. Defining the allocation of responsibilities and obligations for security and privacy between cloud customers and cloud providers—and creating sufficient transparency about that allocation—is a challenge for both industry and government.
- Microsoft understands that strong privacy protections are essential to building trust in cloud computing and allowing it to reach its full potential. We invest in building secure and privacy-sensitive systems and data centers that help protect individual privacy, and we adhere to clear, responsible policies in our business practices—from software development through service delivery, operations, and support.

Comprehensive Privacy Legislation

March 2011

Background

Many countries have comprehensive privacy laws that govern how personal information is collected, used, and shared, and those laws are typically enforced by data protection authorities. In countries that lack such comprehensive national laws (including the U.S.), privacy is governed through a combination of local laws and national 'sectoral laws' that apply to specific industries. In the United States, a growing number of differing local and national laws have created an environment of uncertainty for organizations.

Comprehensive national legislation would help create legal certainty by preempting state or provincial laws that are inconsistent with national policy. It would also help promote both accountability and innovation by ensuring that all businesses are using, storing, and sharing data in responsible ways—while still encouraging companies to compete on the basis of more robust privacy practices.

We believe that government and industry can work together to develop effective, consistent, and constructive privacy protection frameworks that streamline an increasingly complex set of laws governing privacy and data protection. Increase clarity and alignment of regulatory efforts will improve transparency, security, and consistency—and greater consumer control over their personal information.

Microsoft has long advocated for the development and implementation of comprehensive national privacy legislation. We also work with various regional stakeholders to advance the Asia-Pacific Economic Cooperation (APEC) privacy framework. The EU Data Privacy Directive addresses many of these issues in Europe with principles for the collection, processing, and safeguarding of personal data.

Helpful Resources

www.microsoft.com/privacy
Microsoft privacy website, with links to white papers and backgrounders

www.microsoft.com/privacy/cloudcomputing.aspx
Privacy in the Cloud: Read about the evolution of cloud computing and how Microsoft is addressing privacy in this realm.

www.microsoft.com/privacy/bydesign.aspx
Privacy by design at Microsoft

Microsoft's Approach

- Microsoft has been a leading advocate for comprehensive federal privacy legislation since 2005. We believe federal legislation can give consumers control over the collection, use, and disclosure of personal information and greater confidence in their online and offline transactions.
- Microsoft's long-standing commitment to privacy includes principles, policies, and procedures for building privacy protections into our products and services—from development through deployment and operation.
- We share information and ideas about many of the privacy-related legislative proposals that are taking shape around the world. Our efforts include providing information and feedback to the United States Federal Trade Commission (FTC) on its Self-Regulatory Principles for Behavioral Advertising; participating in the European Commission's consultation process for the European Union Data Protection Directive; and supporting the development of the Asia-Pacific Economic Cooperation Privacy Framework.

Policy Considerations

- Microsoft believes comprehensive privacy legislation should apply both online and offline and should include baseline requirements for transparency, consumer control, and security. Legislation also should create legal certainty by preempting state or provincial laws that are inconsistent with federal policy. Finally, it should promote accountability by ensuring that all businesses are responsibly using, storing, and sharing data—while still encouraging competition on the basis of more robust privacy practices.
- Legislation is not a complete solution. While comprehensive legislation can and should create flexible, baseline standards, public policy is unlikely to keep pace with evolving technologies and business models. The most effective approach is to develop a framework of clear and comprehensive laws that work in conjunction with industry self-regulation and best practices, technology solutions, and consumer education.
- Privacy legislation should include safe harbors for companies that comply with local government-approved, self-regulatory programs. Voluntary codes of conduct, which should be developed through open, multi-stakeholder processes, can build upon baseline statutory requirements—and can better address and adapt to emerging technologies and rapidly evolving business models.

Key Points

- In countries that lack comprehensive privacy laws (including the U.S.), local, state, and federal government policymakers must develop solutions to align a growing number of widely varied local and national laws through clear, cohesive, and comprehensive legislation.
- Microsoft has led the call for comprehensive privacy legislation since 2005. We advocate legislation at the national level that allows consumers to have greater control over the collection, use, and disclosure of personal information and a greater sense of security about their online and offline transactions.
- Microsoft believes comprehensive privacy legislation should apply to both online and offline computing and should include baseline requirements for transparency, consumer control, and security. Privacy legislation also should create legal certainty by preempting local laws that are inconsistent with national policy. It should promote accountability by ensuring that all businesses are using, storing, and sharing commercial data in responsible ways. Finally, privacy legislation should continue encouraging companies to compete on the basis of more robust privacy practices.

Microsoft Security Intelligence Report and Privacy

November 2010

Background

The Microsoft Security Intelligence Report (SIR) is a comprehensive evaluation of the evolving threat landscape and security trends, many of which have an impact on privacy. Using data derived from over 600 hundred million Windows computers, as well as some of the largest online services on the Internet, the SIR provides detailed analysis of trends in software vulnerabilities, phishing, password-stealing malware, rogue security software, and other threats.

- **Data Breach Trends** – The number of publicly-reported data breaches has recently declined by about 50 percent, from nearly 400 incidents in the first half of 2008 to fewer than 200 in the first half of 2010. This downward trend may be related to the overall decline in worldwide economic activity over the same time period, or it may reflect improved security practices by organizations regarding sensitive data. The largest single category of incidents involves stolen equipment, accounting for 30.6 percent of all data breaches.
- **Phishing Sites** – Criminals use websites to conduct phishing attacks or distribute malware, often for the purpose of stealing Personally Identifying Information (PII). In the first half of 2010, sites that target financial institutions accounted for the majority of active phishing sites, ranging from 85 to 90 percent of active phishing sites each month.
- **Password stealing Trojans** – The two most commonly detected "families" of malware were Win32/Taterf and Win32/Frethog, both of which are password-stealing **Trojans** – malware used to transmit personal information, such as user names and passwords. These two malware families resulted in nearly eight million detected infections in the first half of 2010.
- **Rogue security software** – Rogue security software, also known as scareware, is software that appears to be security software but provides no real security. Rogue security software often attempts to lure users into participating in fraudulent transactions and attempts to steal personal information. The SIR found over 4 million infections worldwide of rogue security software in the second quarter of 2010 alone. Some versions emulate the appearance of Microsoft products.

Microsoft Approach

- The Microsoft Security Development Lifecycle (SDL) is a security assurance process that is focused on software development. It is a collection of mandatory security activities, grouped by the phases of the traditional software development life cycle (SDLC).
- The Microsoft Security Response Center (MSRC) employs some of the world's top experts on computer security. When a security threat arises, MSRC researchers analyze the risk and distribute security updates. The MSRC also helps customers prioritize their response to new threats.

Helpful Resources

www.microsoft.com/msrc
Microsoft Security Response Center (MSRC) website

www.microsoft.com/sir
Microsoft Security Intelligence Report website

www.microsoft.com/security_essentials
Microsoft Security Essentials

www.microsoft.com/sdl
Microsoft Security Development Lifecycle (SDL) website

www.microsoft.com/mmpc
Microsoft Malware Protection Center (MMPC) website

- The Microsoft Malware Protection Center (MMPC) provides world class anti-malware research and response capabilities that support Microsoft's range of security products and services.
- Microsoft's security website, www.microsoft.com/security, provides extensive guidance and free resources for customers to make their computers less vulnerable to security threats and breaches. This includes Microsoft Security Essentials, a free anti-malware program designed for consumers.
- Microsoft collaborates closely with security researchers and other companies around the world to help protect our customers. We co-founded the Industry Consortium for Advancement of Security on the Internet (ICASI), and the Microsoft Security Response Alliance (MSRA).

Policy Considerations

- Microsoft welcomes the support of governments in fighting online security threats. We believe cooperation with authorities is the most effective means for reducing cyber threats in general, and we support balanced regulation as part of that effort. We believe that less onerous restrictions on industry allow for greater innovation and flexibility in implementing responses to cyber crime.
- Microsoft has joined with industry partners to encourage countries to adopt and ratify the Council of Europe Convention on Cybercrime, which requires signatories to adopt and update laws and procedures to address crime in the online environment.
- Microsoft supports the funding of basic security research by governments in order to help improve the security of online systems.

Key Points

- The Microsoft Security Intelligence Report (SIR) provides an in-depth perspective on the changing Internet security threat landscape, including the latest trend data on data breaches, vulnerabilities, and trends in malicious software that impact privacy.
- The Microsoft Security Response Center (MSRC) employs some of the world's top experts on computer security, and the Microsoft Malware Protection Center (MMPC) provides world class anti-malware research and response capabilities.
- Microsoft welcomes the support of governments in fighting online security threats. We believe cooperation with authorities is the most effective means for reducing cyber threats in general, and we support balanced regulation as part of that effort.

Privacy Use and Obligations

February 2011

Background

The privacy policies implemented by online companies today are largely based on a model of "notice and consent." In this model, a company gives notice to consumers through a privacy statement that describes what information will be collected and how it will be used. The company promises not to use data in a manner that is not consistent with the consumer's choice. Consumers give their consent by agreeing to the privacy statement.

This model is neither well-suited nor sufficient to serve the new information economy. Collection of an individual's personal information has become more widespread, less transparent, and more indirect (through secondary sources as opposed to directly from individuals). Concepts of data usage that underpin traditional privacy governance can break down when information is used for dozens of purposes across many organizations. New technologies and business models that offer benefits to individuals can mean using information in ways that aren't always anticipated when the information is collected. Asking individuals to assume responsibility for policing the use of data in this environment is no longer reasonable, nor does it provide a sufficient check against inappropriate and irresponsible data use in the marketplace. As a result, consumers have the inappropriate burden of responsibility.

The "use and obligations" model is better suited for both the organizations that collect data from individuals and other parties that may also use collected data. The "use and obligations" model places appropriate "obligations" for fair use on all parties, regardless of who collects or holds information. That means every party that uses information has obligations for appropriate data management and transparency; for offering and honoring appropriate consumer choices; for security; and for preventing harm to individuals. Such an approach also emphasizes the need for greater accountability by organizations that manage and share personal data.

The "use and obligations" model in no way lessens the requirement that information be collected in a fair and lawful manner. Rather, it provides a governance approach that is more manageable for businesses and more effective for consumers because it imposes higher obligations on data practices that pose greater privacy risks. As a result, this approach avoids or minimizes impediments to legitimate and necessary collections of consumer information.

Helpful Resources

www.microsoft.com/privacy
An Overview of Microsoft Privacy Policies and Initiatives

www.microsoft.com/privacy/principles.aspx
Microsoft's Privacy Principles

www.microsoft.com/windowsphone/en-us/howto/wp7/web/location-and-my-privacy.aspx
Windows Phone: Location and Privacy Questions and Answers

www.microsoft.com/maps/streetside.aspx
Bing Maps Privacy Questions and Answers

www.microsoft.com/privacy/dpd
Microsoft Data Privacy Day Survey on Location-Based Services

Microsoft Approach

- Microsoft believes the way data is used, rather than how it is collected, is a better basis for defining data protection and privacy obligations related to that data. Microsoft supports an approach that emphasizes "use and obligations" rather than relying on "notice and consent."
- Microsoft recognizes the need for self-regulatory principles governing data usage that provide consumers with greater transparency and control. Microsoft's own practices include commitments to user notice, user control, security, and best practices.
- Microsoft's principles are generally tailored to account for the types of information we collect and how we intend to use that information.

Policy Considerations

- Microsoft encourages the adoption of the "use and obligations" approach to self-regulatory principles that imposes greater obligations depending on the type of online activity involved. We are pleased that this concept is being explored in the context of pending legislative proposals in both the U.S. and Europe.
- The "use and obligations" model can exist with current fair information practices, as well as applicable law. This model in no way lessens the requirement that information be collected in a fair and lawful manner.
- As governments act to address issues associated with emerging technologies and online services, they should not stifle innovation and technology adoption in the process. Government and industry can work together to establish appropriate principles.

Key Points

- The current data protection model of "notice and consent" is inadequate, because increasingly complex uses and reuses of data place too much of a burden on consumers.
- The "use and obligations" model places obligations for fair processing on all parties, regardless of who collected or holds the information.
- Microsoft believes that the way personal data is used, rather than how it is collected, is a better basis for defining the data protection and privacy obligations related to that data.

Online Safety

February 2011

Background

While the Internet provides youth with access to a wealth of experiences in the online world, at the same time, parents face new challenges in monitoring the content their children encounter online, the people they meet there, and what they share. Some key risks facing children online today include:

- **Inappropriate content** – Children are curious and can stumble upon questionable content while searching for something else by clicking a presumably innocuous link in an instant message or blog, or when sharing files.
- **Inappropriate conduct** – Children—and adults too—may use the Internet to harass or exploit other people. Kids may sometimes broadcast hurtful, bullying comments and embarrassing images.
- **Inappropriate contact** – Predators can use the Internet to find and approach vulnerable children. Frequently, their goal is to develop what children believe to be meaningful online relationships and later influence the children to meet in person, a process referred to as "online grooming."
- **Inappropriate commerce** – Children can be tricked into downloading malicious software or revealing personal information for purposes of identity theft by rouge websites run by criminals.

Microsoft Approach

Microsoft's approach to children's online safety includes: **1)** technological tools; **2)** education and guidance; **3)** robust internal policies and practices for moderating content and addressing online abuses; and **4)** partnerships with government, industry, law enforcement, and others to help create a safer, more trusted Internet for all.

- **Technological tools** – Parents can work to minimize online risks by using safety features built into a wide range of Microsoft products and services. For example, Windows Live Family Safety 2011 provides tools that help monitor and protect children online. Microsoft enables all Windows Live ID account holders to specify who can view their profile, contact them through Windows Live Messenger and Hotmail®, and post or view comments about their shared content in Windows Live. In addition, Xbox comes equipped with Console Safety Settings.
- **Partnerships with government, industry, law enforcement, and NGOs** – In our view, creating a safer online environment requires a holistic approach in which consumers, government leaders, technology providers, and non-governmental organizations (NGOs) all play a vital role. A key part of Microsoft's engagement is through public policy with governments around the world.

Helpful Resources

www.microsoft.com/security
Microsoft's online safety and security resource website with aged-based guidelines for Internet use

www.icmec.org
The International Centre of Missing & Exploited Children (ICMEC)

www.fosi.org
Family Online Safety Institute is an international nonprofit organization working to develop a safer Internet

www.getnetwise.org
A project of the Internet Education Foundation, addressing the latest web safety issues and online safety education

- **Robust internal policies and practices** – Company-wide policies, standards, and procedures in the development of Microsoft products and services that connect with the web work to promote online safety. These measures include enforcing a code of conduct for users of Microsoft online services, and moderating content and interactions to address issues such as abuse, illegal activity, and inappropriate material.
- **Education and guidance** – The Microsoft Safety & Security Center, www.microsoft.com/security, provides age-based guidance for Internet use, including tips on how to teach children what's appropriate to view and share online. The site addresses issues including cyberbullying, safer social networking, mobile device safety, tips for responsible online gaming, and how to avoid, block, and report inappropriate behavior.

Policy Considerations

- **Strengthen and enforce laws against child exploitation** – Microsoft works with the International Center for Missing and Exploited Children (ICMEC), INTERPOL, and other organizations to encourage governments to strengthen and enforce laws against the possession and distribution of child pornography.
- **Support industry self-regulation as well as legislative frameworks in emerging technology areas** – As governments act to address risks associated with emerging technologies and online services, it is important that they enable innovation and technology adoption in the process. Government and industry can work together to establish safety principles and provide the means for service providers to help fulfill those promises. Examples include the Safer Social Networking Principles for the European Union and ISP "codes of practice" in Australia, the United Kingdom, and the United States.
- **Promote integration of Internet safety education into school curricula and teacher training** – Microsoft believes that students and teachers can benefit from learning to avoid online dangers, to protect their technology devices, and to conduct themselves ethically on the web. We encourage governments to partner with Internet technology providers, online safety organizations, and school districts to help fill this need using a range of available online safety curricula.
- **Commission studies and fund research to advance Internet safety** – Research is particularly important for identifying factors that increase online risks and for dispelling myths that can lead to misplaced efforts. Government funding for both academic and industry research in these areas is essential.

Key Points

- While the Internet enables many enriching experiences for children, there are also risks, including potential exposure to inappropriate content, contact with bullies or strangers, and loss of privacy.
- Microsoft's approach to children's online safety includes: 1) technological tools; 2) education and guidance; 3) robust internal policies and practices for moderating content and addressing online abuses; and 4) partnerships with government, industry, law enforcement, and others to help create a safer, more trusted Internet for all.
- Online safety is a community challenge, and government and industry should work together to establish and implement online safety principles. As governments act to address risks associated with emerging technologies and online services, it is important that they continue to encourage innovation and technology adoption in the process.

Combating Child Exploitation Online

February 2011

Background

Every day, millions of people connect and share content on the Internet in beneficial and constructive ways. But the Internet has also created new avenues for criminals to exploit young people through means such as distributing child pornography (also known as child abuse images); the sex trafficking of children; or using social networks, chat rooms, and instant messaging for malicious purposes.

The production and distribution of child pornography represents a significant law enforcement problem. Since 2003, the National Center for Missing and Exploited Children® (NCMEC) has reviewed and analyzed almost 30 million images and videos of child pornography. These photos of sexual abuse are seized from pedophiles who trade the illegal images and from communities that reinforce their shared interest in children. Internet companies have an important role to play in the fight against child pornography and can help combat this illegal trade by acting quickly to remove illegal images and developing mechanisms to report abuse to the proper authorities.

Another form of online child exploitation is the use of the Internet by child predators. Predators use the Internet to search for victims. These predators take advantage of the Internet's anonymity to build online relationships with young people or to communicate with those who traffic children for sex. Like the fight against child pornography, Internet companies also have an important role to play in stopping online predators and child sex traffickers, by enforcing codes of conduct, providing mechanisms for customers to report potential predators, investing in innovation for improved detection, and working with law enforcement, government, NGOs and others in the industry to advance solutions to stop child exploitation.

Microsoft Approach

- The Microsoft Digital Crimes Unit is a worldwide team of lawyers, investigators, technical analysts, and other specialists whose mission is to make the Internet safer and more secure through strong enforcement, global partnerships, and policy and technology solutions that help to promote a more secure Internet, defend against fraud, and protect children.
- Microsoft devotes extensive resources to developing technology to combat online child exploitation and supporting the efforts of governments and NGOs in this area. We apply filtering tools and employ more than 100 trained experts to help detect, classify, and report child abuse images transmitted using our online products such as the Bing™ search engine and Hotmail®. Among the latest tools for this purpose is an advanced technology called PhotoDNA, which helps automate and refine the search for child pornography among the billions of photos on the Internet. In 2009, the Microsoft Digital Crimes Unit donated the license for PhotoDNA to the National Center for Missing and Exploited Children to help them work with online service companies to combat child pornography.

Helpful Resources

www.microsoft.com/security
Microsoft's online safety and security resource website with aged-based guidelines for Internet use

www.icmec.org
The International Centre of Missing and Exploited Children (ICMEC)

www.ncmec.org
The National Center for Missing and Exploited Children (NCMEC) in the United States

http://demiandashton.org/
The DNA Foundation

www.microsoft.com/CETS
Microsoft's Child Exploitation Tracking System website

www.microsoftphotodna.com
Microsoft's PhotoDNA project website

- Microsoft reports images of apparent child pornography on its sites to the National Center for Missing and Exploited Children (NCMEC), removes them, and bans the individuals or entities responsible for publishing them from using our services. Microsoft has worked with law enforcement agencies to develop the Child Exploitation Tracking System (CETS), a software tool that allows investigators to share and analyze information related to criminal acts, such as possessing or distributing child pornography, kidnapping, and physical or sexual abuse. CETS is used by law enforcement officers in many locations around the world.
- Microsoft is also working with partners to advance further innovation to fight child exploitation. In September 2010, Demi Moore and Ashton Kutcher's DNA Foundation announced the formation of a technology task force with Microsoft, Facebook, Twitter, Google, and others to explore new ways technology can address the child sex trafficking problem.

Policy Considerations

- Microsoft strongly supports the enactment and enforcement of laws against the production, distribution, and possession of child pornography worldwide. As of 2011, 58 countries have criminalized the possession of child pornography.
- Internet companies should continue to work with governments to help address some of the risks of online predators by establishing industry best practices and guidance.
- Internet companies can help stop the trade in child abuse images online by acting quickly to remove and disrupt the spread of illegal images and by deploying mechanisms for reporting abuse to the proper authorities. Internet companies can help fight online predators by enforcing codes of conduct, providing mechanisms for customers to report potential predators, and by working with law enforcement.

Key Points

- The Internet serves many beneficial and constructive purposes, but it has also created new avenues for criminals to exploit young people, such as the production of pornography.
- Microsoft devotes more than 100 trained experts as well as extensive resources to developing technology to combat online child exploitation, including filtering tools and PhotoDNA, which helps automate and refine the search for child pornography among the billions of photos on the Internet.
- Microsoft has worked with law enforcement agencies in Canada and elsewhere to develop the Child Exploitation Tracking System (CETS), a software tool that allows investigators to share and analyze information related to criminal acts, such as possessing or distributing child pornography, kidnapping, and physical or sexual abuse.

Cyberbullying

November 2010

Background

Bullying among youth has been a serious problem for many years, but technology now provides bullies with new ways to torment their victims, giving rise to the phenomenon of "cyberbullying." The Cyberbullying Research Center in the United States defines cyberbullying as "willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices." Some examples of cyberbullying include: sending hateful or threatening messages online or to a cell phone; posting embarrassing pictures or information about someone online with the intent of humiliating another; impersonating someone online; and disclosing another's private information by forwarding emails and/or text messages.

Youth who experience cyberbullying can suffer damaging mental health consequences and, according to the Cyberbullying Research Center, "research reveals a link between cyberbullying and low self-esteem, family problems, academic problems, school violence, and delinquent behavior. Finally, cyberbullied youth also report having suicidal thoughts."

Estimates of the prevalence of cyberbullying vary, with surveys finding that between 10 percent and 40 percent of youth in the European Union, the United States, and Australia have at one time been victims of cyberbullying.

Recognizing the seriousness of the cyberbullying problem, the online technology industry is partnering with governments, industry groups, and others to help address the problem of cyberbullying through efforts like GetNetWise in the United States and Insafe in the European Union.

Microsoft Approach

- Microsoft enforces policies against abuse and harassment on our online services such as Windows Live Hotmail® and Windows Live Messenger®. Customers who misuse Microsoft services are subject to account termination. Serious incidents may be reported to law enforcement.
- Microsoft provides safety tools like Windows Live Family Safety, which allows parents to monitor their children's Internet use and block unwanted contact in Windows Live Hotmail and Windows Live Messenger.
- Microsoft works with governments, law enforcement agencies, educators, children's advocacy groups, and others worldwide to help create a safer online environment for children by monitoring online services for abuse and by providing safety tools and education.

Helpful Resources

www.microsoft.com/security
Microsoft's Online Safety, Privacy, and Security Education Center

www.getnetwise.org
A comprehensive directory of parental control tools and safety education

www.cyberbullying.us
An extensive site on cyberbullying with research and materials for parents

www.saferinternet.org
An online safety education site created in cooperation with the European Union

www.bullying.co.uk
An online safety education and outreach site in the United Kingdom

explore.live.com/windows-live-family-safety
Microsoft's free Windows Live Family Safety software

www.ikeepsafe.org
An online safety education site with extensive resources for both parents and youth

- Microsoft produces educational programs and materials for educators, parents, and caregivers on responsible Internet use and guidance on how to address online risks as they arise.

Policy Considerations

- Microsoft believes that governments play a vital role in helping to combat harassment and threats online through laws that are thoughtfully written to balance safety and freedom of speech.
- Microsoft supports "safe haven" legislation that encourages companies to moderate online behavior by not holding companies accountable for the actions of online speakers when companies engage in moderation. Examples include Section 230 of the U.S. Communications Decency Act and European Union Directive 2000/31/EC.
- Microsoft supports anti-bullying education for elementary and secondary school students as part of a comprehensive online safety curriculum.

Guidance for Parents and Caregivers

- As with any safety issue, parents should talk with their kids about cyberbullying. Ask your kids what they're doing online and encourage them to report to you any behavior that resembles bullying. Work with them to take action and explain what you will do. Advise your kids not to respond to bullying messages but to save relevant communications in the event the harassment escalates and needs to be reported to your school, Internet service provider, or law enforcement agency.
- Don't tolerate cyberbullying behavior at home. Let your children know they should never, under any circumstances, bully someone. Make the consequences clear.
- Work with your local school to ensure they are creating a culture of safety and have policies in place around responsible use of information and communications technologies among the student body.
- Get help from technology. Turn on the safety features available in most programs and services, such as those in Windows 7®, Windows Vista®, Xbox LIVE®, and the Zune® digital media player, to block bullies.

Key Points

- Cyberbullying is a widespread online problem that can result in damaging mental and physical health consequences for youth, including loss of self-esteem and academic challenges.
- Industry, government, educators, and other groups can best address cyberbullying collaboratively with a combination of education, enforcement, policies, and technology tools.
- Governments play a vital role in helping to combat harassment and threats online through laws that are thoughtfully written to balance safety and freedom of speech.

Freedom of Expression Online

March 2011

Background

Freedom of expression and privacy are fundamental human rights, recognized by societies worldwide. More than ever technological advances, particularly the personal computer and the Internet, make it easier for people to publish and respond to news, information, and opinions. Privacy protections provide an essential foundation for personal well-being, trust, and confidence, both in governments and in technology services. Respecting these fundamental rights is not only good citizenship, it also benefits societies, spurring innovation, academic inquiry, and economic development.

International standards recognize free expression, and privacy rights come with responsibilities and may be subject to regulation in order to further other important goals, such as national security, public safety, and preventing harm to children or to individual reputations. Different governments and societies will have different views on how to integrate these goals, and in our response we strive to take into account local concerns. At the same time, we agree with many in the international community that restrictions on free expression and privacy should only be imposed where necessary, and should be narrowly tailored and provided for by law—and we are opposed to restrictions on peaceful political expression.

Microsoft Approach

- In 2008, we helped form the Global Network Initiative (GNI)—an organization dedicated to advancing Internet freedom—along with other industry leaders, human rights organizations, academics, and socially responsible investors. The GNI has established some basic principles and guidelines for business and is working to discuss these principles and create opportunities for ongoing learning. We are working collaboratively with Google®, Yahoo!®, and the other GNI participants to advance the GNI mission.
- We will continually evaluate our engagement in any market, but where we choose to engage, we will always incorporate respect for fundamental human rights in our approach, express our views to the governments involved, and operate in a principled fashion. The GNI principles and guidelines form the core of our operational approach, which includes:
  - **Responsible company decision-making** – decisions that could impact rights to free expression and privacy incorporate risk assessment and mitigation steps, and involve appropriately senior management;
  - **Minimizing impact** – where laws restrict basic rights to free expression and privacy, we will seek to minimize the impact on protected expression and privacy in fashioning our legal compliance steps;

Helpful Resources

http://blogs.technet.com/b/microsoft_on_the_issues/archive/2010/01/27/microsoft-amp-internet-freedom.aspx
Steve Ballmer, Microsoft, and Internet Freedom

www.gni.org
Global Network Initiative website

» **Transparency and user notice** – we will provide users notice when content is removed, including information on the laws or authorities requiring its removal, and with notice of policies and practices that impact privacy; and

» **Collaboration on learning and public policy** – Microsoft and other companies will continue to engage governments around the world to encourage public policies that respect fundamental rights.

Policy Considerations

- **International Cooperation** – Online freedom is a question of global concern and is not culturally unique to one country or region. Commonly, issues of Internet freedom concern individuals interested in advocating improvements to their own countries, cultures, and communities. Governments should cooperate to improve respect for international human rights principles and to fashion regulations that take account of the Internet's global scope. International cooperation is needed to help protect privacy in cloud computing. As more data moves online, and across borders, we need governments to agree on rules and practices to give consumers certainty and protect civil liberties and privacy.

- **Consider Issues Broadly** – Essential policy goals may at times seem at odds when it comes to Internet freedoms. Government and law enforcement must fight cyber fraud, protect children online, and use all available information to combat terrorism. At the same time, they must respect rights to free expression, privacy, and the rule of law. The Council of Europe has developed important law enforcement-industry cooperation guidelines, which serve as useful guidance in integrating these goals.

- **Support the Ability of People to Connect and to Engage Across Borders** – Internet freedom also includes bridging the "digital divide"—connecting many more of the world's nearly 7 billion people to the information and applications available online. We are working in a wide variety of ways, including through Microsoft Unlimited Potential programs, to help bring technology access to more and more people.

- **Foster Civic Engagement** – Modern societies need to harness the constructive input of citizens in order to make smart policy decisions, foster accountability, and further social trust and stability. Technology, including cloud computing, is driving meaningful improvements in civic engagement and open government. Internet freedoms, by allowing technology to enhance civic engagement, help build better societies and economies.

Key Points

- Online freedom is a question of global concern and is not culturally unique to one country or region. Commonly, issues of Internet freedom concern individuals interested in advocating improvements to their own countries, cultures and communities.

- In 2008, Microsoft helped form the Global Network Initiative ("GNI")– an organization dedicated to advancing Internet freedom - along with other industry leaders, human rights organizations, academics, and socially responsible investors.

- Microsoft will continually evaluate our engagement in any market, but where we choose to engage, we will always incorporate respect for fundamental human rights in our approach, express our views to the governments involved, and operate in a principled fashion.

Online Marketing to Children

March 2011

Background

While the Internet provides children with access to many rich learning and playing experiences online, parents face new challenges and concerns about protecting the privacy of their children online. One concern is ensuring responsible practices for the collection and use of information about children, because many companies that offer online content for children also collect information about them. When children register to join an online site or virtual world, they may be asked to provide their name, email address, age, computing preferences, and other personal information. This information can be used for marketing other products to children.

Parents cannot always monitor their children's use of online services, and they have high expectations for companies to set and enforce secure, transparent, and responsible policies about collecting, using, and storing information about their children. If companies fail to meet these expectations, people will lose confidence in online technologies, and that hurts both industry and consumers alike. That's why Microsoft and other companies with online products and services must adopt particularly strong privacy practices with regard to youth when building their products and services.

Many countries have begun adopting laws and imposing regulations to address the online privacy of children. These approaches, however, are not uniform. Some countries require parental consent; other countries prohibit the collection of certain categories of information even with parental consent. Various countries require different mechanisms for obtaining consent, and in some cases, they require the collection of data that might actually violate privacy regulations in other countries. Forcing companies to comply with conflicting requirements and adapt to differing standards comes at a cost—both financially and through stifled innovation.

Microsoft Approach

- Microsoft incorporates privacy features and parental control technologies into a broad range of our products and services, including Xbox LIVE®, Windows Live™ Messenger, and Hotmail®. Each of these services requests age information in a neutral manner during the registration process. If a child indicates that he or she is under the age of 13, Microsoft obtains parental consent before allowing the child to register and participate in a service's interactive activities.
- When a Microsoft site does collect age information, and users identify themselves as under age 13, the site will either block such users from providing personal information, or will seek consent from parents for the collection, use, and sharing of their children's personal information. We will not knowingly ask children under 13 to provide more information than is reasonably necessary to provide our services, and we do not target advertising to users who we know are under the age of 13.

Helpful Resources

http://privacy.microsoft.com/en-us/fullnotice.mspx#ERBAC
Microsoft Privacy Statement – Collection and Use of Youth's Personal Information

www.microsoft.com/privacy
An overview of Microsoft privacy policies and initiatives

www.microsoft.com/privacy/principles.aspx
Microsoft's Privacy Principles

www.microsoft.com/privacy/principles.aspx
Microsoft comments to the United States Federal Trade Commission regarding the COPPA Rule Review

- Microsoft provides guidance and educational resources for parents, teachers, and children about these important issues. We support a number of educational initiatives that encourage parents to talk to their children about online privacy and that help parents make informed choices about their children's Internet use.

Policy Considerations

- Microsoft supports child privacy legislation that facilitates the free flow of information, builds trust and encourages innovation. Differing standards around the world can stifle innovation by forcing companies to comply with conflicting requirements. Microsoft supports a unified response to public policy and legislation for children's privacy and safety online. Better coordination will ensure that multinational companies can implement an effective and cost-efficient global approach to children's privacy.
- While the concept of age verification systems holds promise for protecting the privacy of children, there currently is no reliable way to verify a child's age online. Microsoft does support measures to improve online identity management, and we are working on technological approaches that might contribute to such improvements.
- In the United States, the Children's Online Privacy Protection Act (COPPA) has helped raise awareness of the importance of protecting child privacy online. COPPA could be improved by clarifying how COPPA works with new forms of online interactions and with methods that are verifiable.

Key Points

- Parents and many governments have concerns about ensuring responsible practices for the collection and use of information about children, particularly from websites that cater to children.
- Microsoft incorporates privacy features and parental control technologies into a broad range of products and services. If a child indicates that he or she is under the age of 13, Microsoft obtains parental consent before allowing the child to register and participate in a service's interactive activities. Microsoft does not target advertising to users who are under the age of 13.
- Microsoft supports children's privacy legislation that facilitates the free flow of information, builds trust, and encourages innovation. Differing standards around the world can stifle innovation by forcing companies to comply with conflicting requirements. Microsoft supports a more unified response to children's privacy and safety online.

Online Safety Education

February 2011

Background

The Internet is an extraordinary tool for enabling children to learn and explore the world around them. Many parents and educators also recognize that "digital literacy" is a prerequisite for their students to compete and thrive in today's increasingly online economy. But while the Internet offers children many benefits, it may also expose them to certain risks, including potential exposure to inappropriate content, contact with bullies or strangers, and loss of privacy. So an education in digital literacy should include learning about those risks and how to avoid them, as well as developing positive online behaviors, such as respect for intellectual property and adherence to basic codes of acceptable conduct.

While governments around the world are investing in technology and related curricula, many schools do not teach comprehensive online safety, even though safety experts identify education as an effective means of protecting children from online risks. Many online safety organizations support comprehensive online safety education as part of the school curriculum.

A comprehensive online safety education curriculum needs to address cyber safety, cyber security, and cyber ethics:

- **Cyber Safety** – Children are taught basic online safety habits and ways to avoid or mitigate potential dangers. They will learn to address issues and when to report problems to the appropriate adult authorities.
- **Cyber Security** – Children are taught how to protect their accounts, identity, and privacy online. They will learn the importance of the need for strong and secret passwords as well as how to update their computers and devices to help protect them from viruses, spam, and phishing scams.
- **Cyber Ethics** – Children are taught how basic citizenship also applies to the online world, including topics such as bullying, plagiarism, and money or identity theft. Children will be given resources to deal with online bullying or harassment, and they will understand the impact their postings or comments may have on others and the consequences of their actions.

Microsoft Approach

- **Microsoft's approach to children's online safety** – Includes **1)** technological tools; **2)** education and guidance; **3)** robust internal policies and practices for moderating content and addressing online abuses; and **4)** partnerships with government, industry, law enforcement, and others to help create a safer, more trusted Internet for all.
- **Partnerships with government, educators, and non-governmental organizations (NGOs)** – Microsoft partners with governments, industry, and NGOs to promote online safety education.
- **Supporting Education** – The Microsoft Safety & Security Center, www.microsoft.com/security, provides age-based guidance for Internet use, including tips on how to teach children what's appropriate to view and share online. The site covers many topics including cyberbullying, safer social networking, using mobile devices more safely, responsible online gaming, and addressing inappropriate online behavior.

Policy Considerations

- **Integration of online safety education in the school curriculum** – A number of jurisdictions have required that online safety education be made an integral part of school systems' efforts to achieve technological literacy for their students. Given the pervasiveness of technology in today's classrooms, Microsoft believes that online safety education is an important component of any school curriculum.
- **Promote online safety as a component of teacher training and professional development** – Just as students need education around safer Internet usage, teachers also need updated guidance and skills to stay ahead of the technology curve. As teachers receive training on how to more use technology effectively in the classroom, they also need to understand current Internet dangers, recognize when students may be subject to online risks, and guide them on conducting themselves ethically on the web.

- **Restriction of online access alone is not a substitute for education** – Regulating children's Internet access may be appropriate in some areas, including instances where age restrictions currently exist in the physical world—like gambling and pornography. But most safety experts agree that access restrictions alone are not enough, and that education needs to play a vital role in online safety.
- **Online safety education should include industry** – Many employees of technology companies are prepared to serve as volunteers to introduce and implement online safety programs. In Australia and the United Kingdom, a program called "ThinkUKnow" pairs Microsoft employees with local law enforcement officials to deliver online safety education and resources to parents, teachers, and children. Industry involvement in online safety education can help achieve greater scale. For example, as part of Safer Internet Day, more than 800 Microsoft employees, from 26 subsidiaries across Europe, reached more than 90,000 teachers, parents, and students with online safety education.

Helpful Resources

www.microsoft.com/security
Microsoft's online safety and security resource website with aged-based guidelines for Internet use

http://ec.europa.eu/information_society/activities/sip/index_en.htm
European Commission Safer Internet Programme

www.staysafeonline.org/in-the-classroom
Online safety tools and materials from the National Cyber Security Alliance in the United States

Key Points

- While the Internet is an extraordinary tool for learning, it may also expose youth to certain risks, including potential exposure to inappropriate content, contact with bullies or strangers, inappropriate conduct such as cyberbullying, and loss of privacy or identity. Comprehensive online safety education is a crucial part of helping to address these risks.
- Microsoft believes online safety curricula should become an integral part of schools' efforts to achieve technological literacy for their students and should include cyber safety, cyber security, and cyber ethics.
- Microsoft supports comprehensive online safety education as part of school curriculum. Legislation requiring schools to implement online safety education should be broad enough to account for local variations in curricula.

Mobile Devices and Youth Safety

March 2011

Background

According to MobileYouthReport.com, it's estimated that, worldwide, 1.6 billion people under age 30 presently own (in 2011) a mobile phone. The benefits are clear: mobile phones allow parents to stay in touch with their children and allow children to connect with their friends—and connect to the Internet with smart phones, which bring a world of information to the palms of their hands.

Mobile phones pose potential safety problems as well. Because many mobile phones provide Internet access, children and young subscribers face the same dangers with a phone as they would with any other Internet-enabled device, including:

- **Inappropriate content –** Young people can be exposed to inappropriate Internet content if they have a smart phone that is Internet-enabled.
- **Inappropriate conduct –** Young people (and adults) may use mobile phones to harass or exploit other people. Children can send hurtful, bullying messages or embarrassing images. A particular concern with mobile devices is "sexting"—the transmission of sexually explicit photographs, which are usually taken with a mobile phone camera.
- **Inappropriate contact –** Predators can use the Internet to find and approach vulnerable children. Frequently, their goal is to develop what children believe to be meaningful online relationships. Predators later persuade children to meet in person—a process referred to as "online grooming."
- **Inappropriate commerce –** Children can easily fall victim to phishing or other scams, and they are more likely to download items such as games or ringtones that result in surprising, expensive charges on mobile phone bills.

Microsoft Approach

- Microsoft's approach to children's online safety includes: **1)** technological tools; **2)** education and guidance; **3)** robust internal policies and practices for moderating content and addressing online abuse; and **4)** partnerships with government, industry, law enforcement, and others to help create a safer, more trusted Internet for everyone.
- Microsoft partners with mobile service providers and independent software companies to give families safety solutions for mobile phones, such as content filtering, usage limits, and contact management.
- Microsoft partners with industry and non-governmental organizations to help promote mobile safety for children and young people. These organizations include the GSM Association®, CTIA – The Wireless Association®, and the Family Online Safety Institute®.

Helpful Resources

www.microsoft.com/security
Microsoft's online safety and security resource website with aged-based guidelines for Internet use

www.fosi.org
Family Online Safety Institute is an international non-profit organization working to develop a safer Internet

www.besmartwireless.com/
Online safety information for parents, educators, and policymakers provided by the U.S. CTIA

www.mobilebroadbandgroup.com
Coalition of mobile providers in the United Kingdom promoting social responsibility

- Before any Windows® Phone application can gain access to location-based information, customers must allow the application to access the device's location (opt-in). Location-based applications must give customers the ability to turn off, or block, program access to their location. Customers can also use phone settings to turn off location-based sharing, and to block all location-based applications and services from accessing location data.

Policy Considerations

- Microsoft supports industry self-regulation and legislative frameworks in emerging technology areas. As governments address risks associated with emerging technologies and online services, they must also ensure that innovation and technology adoption aren't stifled along the way. Government and industry can work together to establish safety principles and provide the means for service providers to help fulfill those promises.
- Microsoft believes the best way to protect children from inappropriate content is the voluntary adoption of content controls, rather than through mandatory filtering or mandatory content ratings.
- Microsoft supports efforts by mobile providers to establish voluntary industry guidelines and best practices to address issues such as content classification, location-based services, and mobile commerce in order to help families make the best, informed decisions.
- Because mobile devices can be effective tools for learning, we encourage governments to partner with information and communications providers, online safety organizations, and school districts to promote safety curricula and address mobile safety.

Key Points

- Mobile phones are widely used by young people in many countries, and they have become an important means of communication for families worldwide. Despite their benefits, mobile phones pose some safety concerns such as inappropriate content, conduct, contact, and commerce.
- Microsoft partners with mobile service providers and independent software companies to provide safety solutions for mobile phones, including geolocators, content filtering, usage limits, and contact management.
- Microsoft supports efforts by mobile providers to establish voluntary industry guidelines and best practices to address issues such as content classification, location-based services, and mobile commerce—and to help customers make decisions that are best suited for their families.

Safer Online Gaming

March 2011

Background

Video and online gaming offers a wide variety of content for many audiences. As with all forms of entertainment, not all content is appropriate for, or acceptable to, all people, and many have expressed concern about the potential harmful effects of violent games on children. Some governments have responded to these concerns by considering restricted access or banning certain video games because of sexually explicit or violent content.

The gaming industry has taken the initiative by adopting voluntary ratings systems, including Entertainment Software Ratings Board (ESRB) ratings in the United States, the Pan European Game Information (PEGI) ratings in the European Union, and the Computer Entertainment Rating Organization (CERO) in Japan. These widely recognized rating systems provide descriptive information about game content, which merchants are encouraged to use, and parents can use these rating systems as guides for buying video games. PEGI is used across more than 30 European countries, and a 2009 survey found that 93 percent of European consumers recognize PEGI labels. A 2010 survey found that 75 percent of U.S. parents "regularly check a game's rating before making a purchase." A "secret shopper" program by the U.S. Federal Trade Commission (FTC) in 2009 found that 80 percent of U.S. merchants refused to sell a mature-rated game to a minor.

Regardless of the brand of entertainment products a family owns—or whether children play games, watch movies, video chat, or interact online—it is vital that parents understand the ever-changing digital world that captivates children's attention and imagination. Parents must understand rating systems for video games, movies, and television and must know how to set parental controls to protect children by limiting Internet access, content, and the amount of time children spend on computers.

Microsoft Approach

- **Technology and tools** – Microsoft is proud of our tradition of industry-leading efforts. We were the first to introduce ratings-based parental controls, called Family Settings, on the Xbox® console, and the Xbox 360® is the only gaming console to offer time management controls. The Family Timer allows parents to set the amount of time that an Xbox 360 console can be used—either per day, or per week. We recently added an Activity Report, which shows parents their children's online activities and facilitates parent-child discussions about video game use.

Helpful Resources

www.GetGameSmart.com
The Get Game Smart program helps families safely enjoy video games and online media

www.microsoft.com/security
Microsoft's online safety and security resource website includes aged-based guidelines for Internet use

www.esrb.org
Entertainment Software Ratings Board

www.pegi.info
Pan European Game Information (PEGI)

www.cero.gr.jp
Computer Entertainment Rating Organization (CERO)

- **Partnering with NGOs, safety advocacy groups, industry, and government** – Microsoft, together with more than a dozen partners—including the Boys and Girls Clubs of America® and the National Center for Missing and Exploited Children®—launched a national outreach campaign in 2009. The "Get Game Smart" campaign encourages parents and caregivers to talk to their children about video games and digital media.
- **Consumer education and outreach** – Our work is incomplete if consumers do not know how to use the technology, tools, and resources that are available to them. It's important to continue educating parents and families about the technology and tools we create for them.
- **Internal policies and practices** – Our efforts to promote safety include developing company-wide policies, standards, and procedures for Microsoft products and services that connect with the Internet. We enforce a code of conduct for customers that use Microsoft gaming services, and we moderate content and interactions to address issues such as abuse, illegal activity, and inappropriate material.

Policy Considerations

- Microsoft supports a vibrant gaming economy that allows game developers and publishers to create products and content for customers of all ages. At the same time, we want to give parents and caregivers the knowledge and tools they need to make informed decisions about the quality and appropriateness of interactive games and programs that their children play and watch.
- Microsoft believes that a combination of voluntary industry rating systems, family education, and parental involvement offer the best solutions for addressing concerns about gaming and entertainment.
- Microsoft supports many efforts to create and enforce laws against child exploitation. We work with the International Centre for Missing and Exploited Children (ICMEC)®, INTERPOL, and other organizations to help governments strengthen and enforce laws to stop the possession and distribution of child pornography.

Key Points

- While the world of gaming offers many enriching experiences for young people, some video games contain mature content, which raises questions about how parents can best protect their children.
- Microsoft's approach to children's online safety includes: technological tools; education and guidance; policies and practices for moderating content and addressing online abuses; and partnerships with government, industry, law enforcement, and others to help create a safer, more trusted online environment.
- Microsoft believes that online gaming concerns can be addressed with a combined approach of family education and involvement, and voluntary industry rating systems, such as ESRB®, PEGI, and CERO.

STOP. THINK. CONNECT.

October 2010

Background

The Internet may be the landmark invention of our lifetime. It offers a new way to work, communicate, learn, play, and grow. But, like the real world, the Internet comes with risk. The digital age has enabled sophisticated new ways of causing harm—to people, their property, businesses, and even nation-states. The vast benefits the Internet offers clearly outweigh the risks, but it's still important to protect people and their valuables. The best way to do this is to make them aware of potential pitfalls and strategies for avoiding them.

Microsoft has invested in consumer awareness about safer use of its products and the Internet for decades, as have others in the industry. Over time, consumer attitudes and behaviors have changed—for the better. For instance, in the early 2000s, most home computer users had never even heard of "phishing," even though the concept had then been around for about 15 years. Phishing occurs when criminals try to trick unsuspecting consumers into giving away valuable personal information via fraudulent emails and phony websites. Today, thanks to heightened public awareness, many consumers know to use caution when clicking links in emails, and recognize dubious email notifications that they're "a winner," or have been selected to receive "a gift" from someone they've never met. Still, more work needs to be done. Phishing is just one type of online scam, and Microsoft and other companies and groups can only do so much when working alone.

In June 2009, the National Cyber Security Alliance (NCSA) and the Anti-Phishing Working Group (APWG) brought together a group of 20 representatives from industry, business, and the non-profit sector. Their goal: to create a simple, actionable message to raise public awareness about online safety and security, which all participants could share and support.

Following a request from the U.S. President for a national public awareness campaign for computing safety and security, the NCSA-APWG-led effort expanded to include the Department of Homeland Security (DHS) and other government agencies and departments.

Launched at the Seattle kickoff of National Cyber Security Awareness Month (NCSAM) 2010 in October, **STOP. THINK. CONNECT.** stands as a prime example of public-private cooperation. It is the result of 16 months of work by coalition members. The campaign is the first step toward building a "culture of online safety," similar to public awareness campaigns aimed at encouraging seat belt use, and the "Smokey the Bear" campaign that encouraged forest fire prevention.

Helpful Resources

www.microsoft.com/security
Microsoft Online Safety, Security, and Privacy Education

www.facebook.com/SaferOnline
Microsoft Online Safety Updates on Facebook

http://stopthinkconnect.org
STOP. THINK. CONNECT. Tips and Advice Page

Microsoft Approach

Microsoft's three-pronged approach to improving Internet safety and security includes:

- Empowering consumers with knowledge and tools to protect themselves, their families, and their personal information when they go online
- Helping to safeguard the Internet environment with cutting-edge technology
- Working to create a global culture of online safety in collaboration with others in industry, business, law enforcement, and government.

Policy Considerations

Microsoft encourages governments—both in the U.S. and internationally—to become involved in the **STOP. THINK. CONNECT**. coalition, and to promote and support the group's work.

We believe cooperation among all stakeholders is the most effective means for reducing Internet threats, and we support balanced regulation that leaves room for innovation and flexibility in responding to online risks.

STOP | THINK | CONNECT™

Key Points

- The Internet is an extraordinary catalyst of innovation, education, and global economic growth, but it is threatened by ever more sophisticated kinds of malicious behavior and outright criminality.
- Everyone—consumers, parents, students, teachers, government, law enforcement, and members of business—has a role to play in making the Internet a safer, more secure, and trusted environment.
- Microsoft teamed with a broad coalition to launch Stop. Think. Connect., a campaign to raise awareness of Internet safety risks and strategies to help keep individuals and organizations safer online.

Safer Social Networking

September 2010

Background

In recent years, the web has undergone a dramatic transformation from largely static web pages to "Web 2.0"—a dynamic, interactive set of "web-culture communities," including social networking services. Social networking services like MySpace®, Facebook®, Bebo®, Orkut®, LinkedIn®, and Windows Live™ are services people can use to connect with others to share information such as photos, videos, and personal messages, or post resumes to potential employers. Social networking services have become an enormously popular Internet destination. The most popular services have hundreds of millions of members. Unfortunately, the popularity of social networking services has also attracted criminals who attempt to infect computers and steal personal information. So it's important that consumers understand the risks and take appropriate steps to help protect themselves and their digital assets.

Social networking services raise additional issues regarding youth, as many young people draw little distinction between real life and the online world. They may use social networking services designed for children such as Webkinz™ and Club Penguin™, or social networking services designed for general audiences such as YouTube®, MySpace, Flickr®, Twitter, and Facebook. It is important that children understand that many social network profiles can be viewed by anyone with access to the Internet. Kids can use these sites to chat, play games, post and browse photos and videos, blog, and post an online profile. Unfortunately, some of the information kids post on their pages can also make them vulnerable to phishing scams, cyberbullying, and inappropriate contact with adults..

Guidance for Consumers

- Evaluate a prospective social networking service before you use it. Does it offer the level of control, protection, and overall experience that's right for you? Will you feel comfortable in this community?
- Assume that everything you put on a social networking site is permanent. Even if you can delete your account, anyone on the Internet can easily print photos or text and save images and videos to a computer.
- Think twice about who you accept as a friend. Consider adding only those you or close friends have met in person or with whom you have friends in common.
- Use caution when you click links that you receive in messages from your friends on social networking services.
- Educate yourself about social networking services children may be using. Evaluate the sites that they plan to use, and make sure both you and the child understand the privacy policy and the code of conduct. Find out if the site monitors content that people post. Also, review the child's profile periodically.
- Ensure kids follow age limits on the site. The recommended age for signing up for social websites is usually 13 and over.

Guidance for Governments

Social networking services offer great benefits to consumers that are just being realized. Along with these benefits come privacy, safety, and security needs that technology companies take very seriously and are a broad industry responsibility. Social networking service companies should continue to work with governments to help address some of the risks by establishing industry best practices and guidance. Some examples of where industry and government have collaborated to help protect consumers are:

- **The Safer Social Networking Principles of the European Union** – a set of best practices agreed upon by 18 social networking service companies, including Microsoft, and the European Union.
- **The Joint Statement on Key Principles of Social Networking Safety** – announced by the United States Attorneys General Multi-State Working Group on Social Networking and MySpace, which resulted in the landmark Internet Safety Technical Task Force report on Enhancing Child Safety and Online Technologies.

Microsoft Approach

As in the physical world, social problems such as predation, bullying, and theft exist online and in social networking services. Microsoft works to address these problems in three primary ways: by developing technology; providing guidance and educational resources; and working with others in collaborative and innovative ways.

- **Technology** – Technology plays an important role in helping to keep consumers safer online. That's why

Microsoft has made a number of advancements to protect its customers better online through technology. Among our free technologies available to consumers are:

  - » **Windows Live Family Safety** – which includes safer social networking features.
  - » **Microsoft Security Essentials** – which provides real-time protection for home PCs against viruses, spyware, and other malicious software.

- **Guidance** – To best protect themselves against online threats, individuals should be armed with more than just the latest technology solutions. Since awareness and education are the first defense in avoiding online risks, Microsoft has made free advice easily accessible on its Website, www.microsoft.com/security. These resources and materials help people have a more secure Internet experience; assist parents in learning how to minimize risks like cyberbullying; and help teach kids how to use social networking sites more safely.
- **Partnering with government, industry, and non-governmental organizations** – The Internet is a safer place for all when industry works together to help protect people. In adherence to this belief, Microsoft frequently works alongside its industry peers, government, and non-governmental organizations to help make the Internet safer.

Helpful Resources

www.microsoft.com/security
Microsoft's online safety and security resource website with aged-based guidelines for Internet use

www.icmec.org
The International Centre of Missing & Exploited Children (ICMEC)

www.fosi.org
Family Online Safety Institute is an international nonprofit organization working to develop a safer Internet

www.getnetwise.org
A project of the Internet Education Foundation, addressing the latest web safety issues and online safety education

Key Points

- Social networking services are a great way for people to connect with friends and family across the Internet to talk, share news and photos, play games, or even search for a job.
- As the popularity of social networking services has grown, so have the risks of using them, including exposure to malicious software, potential loss of privacy, harassment, cyberbullying, and damage to reputation.
- Consumers can help protect themselves and their children by getting educated about some of the risks involved in social networking and by using technologies such as antivirus software and parental controls.
- Governments should continue to work with industry to encourage the benefits and mitigate the risks involved in social networking services by jointly establishing industry best practices and guidelines.

Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • USA