Microsoft

POLICYMAKER GUIDE TO SECURITY, PRIVACY, AND SAFETY

BUILDING GLOBAL TRUST ONLINE VOLUME 3

Advances in computing and communications technologies have made life more connected and more convenient than ever before. Online services now extend to many aspects of everyday life—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, security, and safety often top the list of concerns of policymakers, individuals, large organizations, and governments the world over. The technological tools created for the betterment of society are also being used as instruments for crime and malicious intent, and criminals and irresponsible businesses are a serious cause for concern.

Microsoft's approach, Trustworthy Computing, is a long-term, collaborative effort to create and deliver secure, private, and reliable computing experiences for everyone. Bill Gates launched the initiative in 2002 with an email that announced it to all Microsoft employees.

Since then, important changes have occurred that have led Microsoft to refocus Trustworthy Computing. New threats have presented challenges to computer security professionals. People are now connected through a host of Internet-enabled applications, creating massive new global data flows that strain the traditional notice and consent model that currently protects privacy. Online safety research since 2002 has shown that the Internet is less risky for youth than once thought, and a new consensus is emerging around online safety programs centered on the notion of digital citizenship.

As a signatory to the UN Global Compact, Microsoft is committed to respecting all of the human rights described in the Universal Declaration of Human Rights; the International Covenant on Civil and Political Rights; the International Covenant on Economic, Social and Cultural Rights; and the ILO Declaration on Fundamental Principles and Rights at Work. Microsoft recognizes that as a leading technology provider with global operations, business can help to promote—or be used to impede—human rights. The stakes grow higher every year as information and communications technologies become ever more important in how people work, learn, and interact with one another. Microsoft recognizes the important responsibility to respect human rights, and aims to bring the power of technology to bear to promote respect for human rights throughout the world. Microsoft's full Global Statement on Human Rights is available at **aka.ms/Human-Rights-Statement**.

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

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

- Current online privacy issues and practices.
- Issues related to protecting 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.
- Microsoft's efforts in the area of accessible technology.

This material is intended for any decision maker with responsibility for developing new ideas and solutions for online privacy, security, and safety.

As with any publication intended for a global audience, this information is provided with the understanding that every region will have different priorities, concerns, and ideas for solutions. That's why an open exchange of ideas and information to develop effective global policies and practices is so important—and that solutions must be widely socially acceptable and meet with public approval, especially when balancing security and privacy.

Today's world of digital dependence presents new challenges and concerns that cannot be met or addressed in isolation. The cooperation of businesses, governments, non-governmental organizations, and consumers from around the world is the most effective means of reducing cyber threats. Microsoft supports new frameworks for international cooperation, models for information sharing, and public-private partnerships as part of that effort to create a more trusted personal computing experience and a safer, more secure Internet.

What’s inside

SECURITY

PRIVACY

SAFETY

February 2013

Microsoft Trustworthy Computing

Key Points

- Microsoft is committed to helping create safer, more trusted computing experiences. The company's approach is called Trustworthy Computing, a long-term, collaborative effort to create and deliver secure, private, and reliable computing experiences for everyone.

- Microsoft believes that technology should adhere to business practices that promote trust. Microsoft acts according to the principle that the technology industry should focus on solid engineering and best practices to ensure that the delivered products and services are more reliable, secure, and trusted.

- Microsoft supports collaboration among 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.

BACKGROUND

The Internet allows people to enrich their lives, build commerce, and communicate 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, Trustworthy Computing, is a long-term commitment and collaborative effort to create and deliver secure, private, and reliable computing experiences for everyone. As the Internet becomes increasingly critical to the computing ecosystem, Microsoft is also advancing the company's vision of End to End Trust.

Microsoft believes fundamentally that sensitive data and personal information must be protected and that technology should adhere to business practices that promote trust. Microsoft acts according to the principle that the technology industry should focus on solid engineering and best practices to ensure that the products and services they deliver are more reliable, secure, and trusted. Microsoft supports collaboration among technology companies, governments, consumers, and businesses to solve the security challenges of today and tomorrow.

SECURITY

Microsoft focuses on innovation in secure software development. The Microsoft Security Engineering Center helps to protect Microsoft customers by delivering more secure products through the Microsoft Security Development Lifecycle (SDL). The Microsoft SDL is Microsoft's security assurance process for software development that builds security into every phase of software development and provides defense-in-depth guidance and protection. Microsoft shares the SDL with the software industry to help build safer, more trusted computing experiences for everyone.

- Microsoft's Security Science team performs research that helps to understand online attacks and techniques.

- The Microsoft Malware Protection Center analyzes malicious software and develops solutions that are used in Microsoft security technologies.

- The company also produces the Microsoft Security Intelligence Report, which analyzes the threat landscape of exploits, vulnerabilities, and malware using data from Internet services and over 600 million computers worldwide.

- In the event a vulnerability in Microsoft software is discovered, the Microsoft Security Response Center monitors the situation and responds to the incident. It also manages the security update release process company-wide, and serves as the single point of coordination and communication for these matters.

PRIVACY

- Microsoft regards customer trust as critical to business success and regards protecting privacy as a foundation of that trust. 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 products and services.

- Microsoft builds privacy-enhancing technologies into products and services to help consumers protect their personal information.

- To help organizations more effectively manage the data in their possession, Microsoft provides guidance, frameworks, and technologies that are 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 cloud computing, 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 working to strengthen the reliability of cloud computing by reengineering key products such as Microsoft Exchange Server and Microsoft SharePoint Server to work better as cloud services. Microsoft is also 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. The company works with law enforcement agencies by providing them with technical training and in the development of new technology tools to help combat cyber crime. Microsoft has also assisted in protecting consumers through legal action to thwart 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.

Helpful Resources

Microsoft Trustworthy Computing
www.microsoft.com/twc

Microsoft Safety & Security Center
www.microsoft.com/security

Microsoft Security Response Center
www.microsoft.com/msrc

Microsoft Security Intelligence Report
www.microsoft.com/sir

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

February 2013

Trustworthy Computing Next

Key Points

- In 2002, Bill Gates outlined three key tenets that still define trustworthy computing today: security, privacy, and reliability. But the role of computers in everyday life is changing, and each of these aspects must be fundamentally redefined to meet new challenges.
- Security models need to take a more holistic approach that encompasses prevention, detection, containment, and recovery. Privacy governance needs to replace the current notice and consent model with a framework based on use. Reliability models need to supplement the traditional reliance on data replication and redundancy with a new engineering intelligence that focuses on software that detects, isolates, and repairs outages.
- Governments have a special role in advancing trustworthy computing because they have both the power to catalyze markets through incentives and the ability to dictate behavior through regulation. Governments should also work to establish rules for sharing public and private data and for international access of data by government.

BACKGROUND

On January 15, 2002, Bill Gates sent an email to all Microsoft employees announcing Trustworthy Computing, defining its key tenets as security, privacy, and availability (which is now referred to as reliability).

Since 2002, important changes have occurred in these three areas. New threats and cyber warfare have challenged computer security professionals. People are now connected through a host of Internet-enabled applications, creating massive new global data flows that strain the traditional notice and consent model that protects privacy. Reliability must be improved to accommodate the greater dependence on cloud computing, with large-scale systems promising anywhere, anytime access.

The core attributes of trustworthy computing are as important as ever, but this new set of challenges requires innovative solutions, which Microsoft refers to as Trustworthy Computing Next.

- To meet the security challenges of increasingly determined and persistent adversaries, organizations should adopt a holistic security strategy that encompasses prevention, detection, containment, and recovery.
- To adjust to the privacy implications of a data-rich world, organizations need to craft principles that protect privacy while reaping the benefits that only the massive aggregation of computer data (sometimes referred to as big data) can bring.
- Finally, to build the reliability that information and communications technology (ICT) depends on, organizations need to recognize the complexity of evolving ICT systems, and create products and services that can be flexible in times of failure.

MICROSOFT APPROACH

Trustworthy Computing Next addresses the changes to the online world in each of the three aspects of trustworthy computing: security, privacy, and reliability.

- **Security.** Threats can challenge almost any part of an ICT system, making absolute security impossible. This more dangerous threat environment requires a new model of computer security that consists of prevention, detection, containment, and recovery. While these elements are not new, many organizations have not dedicated their efforts to the strategies necessary to ensure that if part of the network is compromised, the adversary is well contained. Security strategies have also not focused on capturing, correlating, and analyzing audit events from across an enterprise to detect anomalies that reveal attacker movement.

- **Privacy.** It is clear that the privacy challenges in a cloud-enabled world cannot be addressed by traditional privacy principles that focus on the collection of data and the notices provided at the time it is collected—a notice and consent privacy model. The use of data serves as a better starting point for defining the obligations related to personal information. A model based on use is better suited for both the organizations that collect data from individuals and others who may use it. This model requires organizations to be transparent, offer and honor appropriate choices, and ensure that they assess and manage the risks to consumers related to the use of their data.

- **Reliability.** With technology embedded in so many aspects of everyday life, reliability must achieve a level not possible today. To bring this about, two fundamental changes must occur. First, companies must leverage the cloud and its big data to create engineering intelligence—the ability to understand both internal and cross-organizational dependencies. For example, simply watching data flows between networks may reveal significant dependencies that were previously not understood.

  Second, organizations need to stop thinking of reliability solely in terms of redundancy and data replication, which are insufficient to ensure high levels of reliability in the cloud. The traditional emphasis placed on preventing failures in software needs to be supplemented by an increased focus on software that detects, isolates, and repairs (or works around) failures associated with composite computing systems.

POLICY CONSIDERATIONS

- **Government's special role in protecting the Internet.** Governments have both the power to catalyze markets through incentives and the ability to dictate behavior through regulation. Governments also play a unique role in responding to online threats from enforcing criminal laws to protecting a nation from military attacks.

- **Establish rules for sharing public and private data.** Because many cyber attacks impact both public and private infrastructure, the need for a public-private partnership is clear even though the rules for sharing critical information are not. Government and industry must work to create effective mechanisms for sharing data that enhance security.

- **Establish rules for international data access by governments.** Governments need to agree upon a new framework for international assistance that goes beyond traditional mutual legal assistance treaties (which say that the country where data sits has jurisdiction over that data). Under a new framework, countries could agree that there should be a formal process for accessing data.

Helpful Resources

Microsoft Trustworthy Computing Next
www.microsoft.com/twcnext

February 2013

Collective Defense: Applying Public Health Models to Internet Security

Key Points

- Malware and botnets enable cyber crime, costing consumers and business billions of dollars each year. In response, a collective defense across the Internet is needed to ensure a systematic approach to dealing with these threats. Improving the health of consumer devices connected to the Internet will benefit not only consumers, but the information technology ecosystem as a whole.
- One way to address issues of online security is to apply a model similar to the one society uses to address human illness. The public health model of identifying and controlling infectious diseases encompasses a number of concepts that can be applied to Internet security.
- Any effort to promote Internet health and security must be balanced with considerations of the social, legal, and economic issues of privacy, and designed not to impact economic activity adversely. An Internet health model will work as a collective defense only if it is accepted by society and if people are confident that their privacy will be protected.

BACKGROUND

Advances in online 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. Unfortunately, these advances have been accompanied by a rise in online crime, which threatens to undermine the public trust. 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, having little in common in terms of origin, path, or impact. This calls for a myriad of responses and solutions worldwide.
- Botnets, the most insidious of malware, threaten infrastructure, and in turn endanger financial markets, military institutions, and national security.
- Individuals and organizations have a wide variety of choices to help defend their devices against cyber threats, including antimalware solutions, firewalls, and security updates. However, despite the broad availability of these technologies, they are not always fully deployed. Enterprises spend a great deal of time and money to manage risk with well-trained staff and sophisticated systems. Consumers, on the other hand, often lack the expertise and know-how to protect their devices themselves.

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

To improve the security of the Internet, governments and industry could similarly engage in systematic activities to improve and maintain the health of devices connected to the Internet. They could deploy people and technology to promote preventive measures, detect infected devices, and notify affected users. They could then help users repair malware-infected devices and take additional action to ensure that infected computers do not put other computers at risk.

Industry and governments have already begun such efforts. For example, the Internet Industry Association of Australia launched its voluntary Internet Service Provider (ISP) Code of Conduct. ISPs that use this system notify consumers with infected computers and offer them disinfection and repair tools. In Germany, the Anti-Botnet-Advisory Centre works in a similar way with local ISPs who notify and assist consumers whose computers are infected with malware. In Finland, TeliaSonera, an ISP serving 164 million customers, deploys an automated monitoring system to identify infected devices, alert their owners, and quarantine the devices from the network until they are cleaned.

MICROSOFT APPROACH

- Microsoft supports a collective cyber security defense similar to a public health model that limits the spread of human illness. Microsoft believes a similar model can be used by governments and IT industry leaders to more methodically prevent, detect, and treat computers infected with malware or botnets.
- This model is just a starting point. This vision can become a reality only with the support of consumers, government leaders, and privacy advocates, as well as ISPs and others in the industry.
- Microsoft works with the IT community to share information on malware and botnets, and to help assist affected customers.

POLICY CONSIDERATIONS

- Citizens the world over face more dangers online, while businesses and governments confront substantial cyber security issues. These call for collaborative solutions. Effective and far-reaching goals can be achieved only 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 sensitivities, so solutions must be socially acceptable and meet with public approval—especially when balancing security and privacy. Global progress on creating a safer online world merits coordination among industry, government, academics, and all societies worldwide and an open exchange of ideas about how better to protect the health of devices on the Internet.

Helpful Resources

Microsoft Global Security Strategy and Diplomacy Internet Health Site
aka.ms/gssd-health

Microsoft End to End Trust—Internet Health
aka.ms/internet-health

The Internet Health Model for Cybersecurity. EastWest Institute, 2012
www.ewi.info/internet-health

February 2013

Combating Botnets

Key Points

- Botnets are networks of compromised computers, controlled by remote attackers that perform such illicit operations as sending spam, facilitating fraud, or attacking other computers.

- Botnets are of concern to governments and businesses because they can harness large numbers of individual computers to direct an attack against the information technology infrastructure. By working with industry to fight botnets and by passing thoughtful, balanced regulation, governments can help protect their systems and citizens from botnet malware.

- Microsoft aggressively fights botnets by collaborating with governments and others to take them down. Microsoft also provides security tools and guidance to businesses, governments, and consumers.

BACKGROUND

A botnet is a network of compromised computers that can be illicitly and secretly controlled by an attacker without the knowledge of their owners, and then used to perform a variety of illegal actions. Computers in a botnet (also called nodes, bots, robots, or zombies) are usually ordinary computers in homes and offices around the world. A computer becomes a node in a botnet when attackers manage to install malicious software on it, often by using social engineering tactics that trick users into installing it.

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 send spam, host or distribute malware or other illegal files, or attack other computers.

Botnets pose a more dangerous threat than individual hackers to the information technology systems of enterprise and governments because botnets harness large numbers of computers that can be used to direct an attack. The raw computing power of botnets enables them to take down major websites and email servers, as well as other essential parts of critical communications, data, and electronic systems.

Additionally, botnets can pose a threat to IT supply chains. A 2012 Microsoft study found that cyber criminals infiltrated unsecure supply chains using the Nitol botnet, which introduced counterfeit software embedded with malware for the purpose of secretly infecting computers before they were even purchased. Botnets can also provide anonymity to the criminals who control them (known as *botherders*) by enabling them to hide the true source of their attacks behind their widespread network of computers.

MICROSOFT APPROACH

- Microsoft is determined to help fight cyber crime through technology innovation, legal action, and consumer education.
- Microsoft supports governments and law enforcement by giving them technical training, investigative and forensic assistance, and the continued development of new technology tools to combat cyber crime.
- The Microsoft Active Response for Security (MARS) initiative combines legal and technical acumen to proactively disrupt criminal infrastructure. This includes using private legal action and technology measures to take down botnets, seizing the infrastructure and domains criminals use to control them, and taking the information gained in those efforts to better protect the Internet community.

  Project MARS is a joint effort of the Microsoft Digital Crimes Unit, Microsoft Malware Protection Center, Customer Support Services and Trustworthy Computing. Recent examples of MARS successes include disruption and remediation of the Waledac, Rustock, Kelihos, Zeus, Nitol, and Bamital botnets.

POLICY CONSIDERATIONS

- **Public and private partnerships.** Microsoft welcomes the support of governments and law enforcement in fighting botnets. The company believes that cooperation with authorities is the most effective means for reducing cyber threats, and supports balanced regulation as part of that effort. This includes initiatives like the Anti-Bot Code of Conduct for Internet Service Providers recommended by the U.S. Federal Communications Commission. The company also believes that less onerous restrictions on industry allow for greater innovation and flexibility in implementing responses to cyber crime.
- **International cooperation.** Microsoft has joined with industry 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 online crime.
- **Strong enforcement and balanced regulation.** Microsoft strongly supports the enactment and enforcement of laws to combat botnets and the prosecution of cyber criminals. At the same time, it is important that these laws enable innovation and support the adoption of new technology.

Helpful Resources

The Microsoft Safety & Security Center offering security guidance
www.microsoft.com/security

The Microsoft Digital Crimes Unit
www.microsoft.com/dcu

February 2013

Cyber Security

Key Points

- Cyber security is the set of activities and resources that enable citizens, enterprises, and governments to meet their computing objectives in a secure, private, and reliable manner. Governments face the challenge of developing security practices that address four types of threats: conventional cyber crimes, military espionage, economic espionage, and cyber warfare.
- Microsoft works to help create safer, more trusted computing experiences by continually improving the security of its products and services, developing best cyber security practices, and collaborating with governments and industry partners to reduce threats to cyber security.
- An effective approach to cyber security requires collaboration between the public and private sectors to mitigate threats and vulnerabilities. This collaboration also helps develop sustainable public policy frameworks that advance cyber security and enable innovation in the private sector.

BACKGROUND

Cyber security covers the security of information, operations, and computer systems. It is the set of activities and resources that enables citizens, enterprises, and governments to meet their computing objectives in a secure, private, and reliable manner.

Cyber security means different things to different audiences. For businesses, cyber security is about ensuring, through operational and information security, the availability of critical business functions and the protection of confidential data.

For governments, it is about protecting citizens, enterprise, critical infrastructure, and government computer systems from attack or compromise. Governments face the challenge of developing cyber security best practices that address four categories of threats that have the potential to affect public safety and national security.

First, they must protect society from a broad range of conventional cyber crimes, such as fraud or vandalism, perpetrated by individuals, organized crime syndicates, and loosely affiliated groups of "hacktivists." Next, countries may need to combat military espionage that uses computing technologies, as illustrated by repeated allegations of cross-border exfiltration of sensitive military data. Nations must also defend against economic espionage and other such actions where governments have philosophical differences about what constitutes acceptable behavior. Finally, governments must grapple with cyber warfare, forcing a reassessment of traditional notions of war.

With societies around the globe growing ever more dependent on information and communications technologies, the imperative of cyber security will grow significantly over time. Accordingly, policymakers should think strategically about mitigating cyber threats.

MICROSOFT APPROACH

As a business, Microsoft manages risk through ongoing efforts to enhance security in product development, the supply chain, and operations, as well as deepen its understanding of social engineering tactics.

- **Enhancing security in product development.** To address product vulnerabilities, Microsoft uses its Security Development Lifecycle, a security assurance process that relies on a collection of mandatory security activities grouped by the phases of traditional software development.

- **Enhancing security in the supply chain.** To help manage risks to Microsoft's products and services in the supply chain, the company deploys identity and access management controls, the Security Development Lifecycle, policies and procedures that monitor the integrity of Microsoft software, and anti-counterfeit measures.

  Microsoft is also actively involved in industry efforts to develop both best practices for managing risk in the supply chain, and product assurance tools such as the Software Assurance Forum for Excellence in Code (SAFECode).

- **Enhancing operational security.** To help organizations better manage operational security risks, Microsoft shares its security best practices and provides regular software updates. Microsoft's patch management system, with its automated releases for the second Tuesday of each month, enhances operational security through standard, predictable, and regular releases of software patches.

- **Enhancing security against social engineering.** Microsoft helps combat social engineering by sharing its security best practices and developing instructional materials for consumers. It also provides tools like the Windows Internet Explorer SmartScreen Filter, which helps to protect people from evolving social engineering threats.

Building on various internal risk-management programs, Microsoft continually seeks to improve the efficiency and effectiveness of these risk-management approaches. Microsoft shares those practices with industry and policymakers as appropriate.

In addition, Microsoft's Global Security Strategy and Diplomacy team partners with national governments, industry partners, and nonprofit organizations to enhance the security of the Internet. To that end, the team promotes trustworthy plans and policies, and helps protect processes key to national and economic security as well as public health, safety, and confidence.

POLICY CONSIDERATIONS

- Governments should work with the private sector to strengthen the security, privacy, and reliability of the cyber ecosystem and to defend against cyber threats. Microsoft believes that such strategic partnerships and outcome-focused initiatives are critical to advancing a safer Internet.

- In partnership with the private sector, policymakers should build on industry best practices for risk-based, technology-neutral approaches to mitigating cyber threats. When policymakers rely upon tested frameworks, they help ensure that hard-won security gains are maintained and technological innovations are given maximum opportunity to succeed.

- As governments work to advance their national security goals through effective cyber security, they should also consider their unique information technology infrastructures. Public-private partnerships can help identify gaps between national security expectations and what commercially available technologies can offer to address areas of specific concern.

Helpful Resources

Microsoft Global Security Strategy and Diplomacy
www.microsoft.com/gssd

Rethinking the Cyber Threat: A Framework and Path Forward
aka.ms/cyber-threat

Microsoft Security Intelligence Report
www.microsoft.com/sir

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

Microsoft for Public Safety & National Security: Malicious Software Crimes
aka.ms/DCU-economic-crime

February 2013

Cybersecurity Norms

Key Points

- The private sector, with its global supply chain and customer base, can make an important contribution to the emerging discussion of cybersecurity norms.

- As governments continue to develop their views on cyber security and normative behavior in cyber space, creating international public-private partnerships can help ensure the resiliency of critical infrastructures and agility in responding to complex security events in cyber space.

BACKGROUND

"The last two decades have seen the swift and unprecedented growth of the Internet as a social medium; the growing reliance of societies on networked information systems to control critical infrastructures and communications systems essential to modern life; and increasing evidence that governments are seeking to exercise traditional national power through cyber space." [1]

The technology landscape in cyber space is indeed changing rapidly, but agreed-upon standards for state behavior have not kept pace—which in turn raises concern about potential conflicts. (According to the United Nations, more than 30 countries have developed military doctrines related to the use of cyber space and some have developed cyber defense centers.) Developing a global understanding of cybersecurity norms will be critical to the long-term stability, reliability, and security of the Internet and cyber space.

To date, most international discussions on cyber security have taken place among governments through such organizations as the United Nations Government Group of Experts and the Organization for Security and Cooperation in Europe.

However, the technology industry creates and operates most of the infrastructure that enables the Internet today. Industry continues to innovate, build best practices, and set technical cybersecurity norms. These include managing the disclosure of software vulnerabilities, implementing the secure development of software and hardware, swift responses to security incidents, and management of security risk. And during actual cyber incidents, it is the private sector that is critical to effective incident response, often relying on trusted communities of engineers, network operators, and other experts from outside of government.

Global conversations on cyber security would benefit from a private sector perspective that can help governments think through the technical challenges and priorities involved in securing billions of Internet users around the world. Many industry practices could be used as the impetus for public-private partnerships to develop cybersecurity norms, because neither governments nor the private sector can address these challenges alone.

[1] *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, The White House, May 2011.
aka.ms/WhiteHouse-cyberspace

MICROSOFT APPROACH

- Microsoft is committed to supporting discussions on the evolution of cybersecurity norms through partnerships. As governments continue to develop their views on cyber security and normative behavior in cyber space, creating international public-private partnerships can help ensure the resiliency of critical infrastructures and agility in responding to complex security events in cyber space.
- The Microsoft Global Security Strategy and Diplomacy team partners with national governments, industry partners, and nonprofit organizations to contribute to the international discussion of cybersecurity norms.

POLICY CONSIDERATIONS

- **Appropriate forums**. Effective discussions to develop cybersecurity norms take place when governments identify appropriate forums for such discussions. The membership of these forums must include the relevant government stakeholders, have the ability to integrate input from the private sector, and have the expertise necessary to sustain meaningful progress.
- **Public-private partnerships**. To be effective, governments must develop cybersecurity norms in collaboration with the private sector, which owns the majority of today's global networks. Although governments are the primary actors in international negotiations, the private sector can contribute considerable operational experience to help inform their discussions.
- **Focus on consensus**. Governments should focus on areas where achieving consensus in the short term is practical. For example, it may make sense to seek agreement on areas of specific common interest, such as how to deter threats to critical infrastructures, before discussing areas complicated by significant national and cultural differences.

Helpful Resources

Microsoft Global Security Strategy and Diplomacy
www.microsoft.com/security/gssd

Cybersecurity Norms and the Public Private Partnership: Promoting Trust and Security in Cyberspace
aka.ms/norms-public-private

Cybersecurity Norms for a Secure Cyber-Future
aka.ms/Secure-cyber-future

Developments in the Field of Information and Telecommunication in the Context of International Security (UN First Committee)
aka.ms/UN-cyber-security

February 2013

Critical Infrastructure Protection

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.
- The Microsoft Global Security Strategy and Diplomacy team works with national governments, industry, and nonprofit organizations to strengthen and improve cyber security, promote trustworthy plans and policies, and help protect key processes and functions for national and economic security, and public health, safety, and confidence.

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 threats to complex critical infrastructures require an unprecedented response. Technology vendors, governments, and businesses must work together to innovate, develop, and deploy effective solutions. Microsoft is dedicated to supporting these relationships and plans to help detect and preempt the sources of threats to critical infrastructure. As part of that commitment, the company formed the Global Security Strategy and Diplomacy team.

MICROSOFT APPROACH

The Global Security Strategy and Diplomacy Team is dedicated to enhancing the security and resiliency of critical infrastructures by increasing the trustworthiness of software and IT services, in part through the development of innovative solutions. In addition, the team collaborates with governments and critical infrastructure owners and operators to reduce and manage risks.

Effective efforts to protect critical infrastructure fall within these 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. Microsoft collaborates to develop effective, flexible, and innovative national and global solutions to help secure critical infrastructure.

- **Resilient operations.** Microsoft helps 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.

- **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

Leaders worldwide are concerned about the security implications of increasingly interrelated global systems, especially economic stability, climate change, and national security. The potential exists 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 relationships must develop robust plans to secure and protect 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 relationships 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 information technology security research:** solving existing problems and preparing for those in the future by strengthening the pipeline of academic and professional knowledge through educating, mentoring, and training future professionals and leaders.

Helpful Resources

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

Microsoft Global Security Strategy and Diplomacy
www.microsoft.com/security/gssd

The Industry Consortium for Advancement of Security on the Internet
www.icasi.org

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

February 2013

Data Breach Notification

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.

- Because Microsoft is committed to helping create safer, more trusted computing experiences, it is dedicated to protecting sensitive data and personal information. It recommends a multifaceted approach to data governance that includes policy, people, processes, and technology. Microsoft's approach relies on creating or maintaining more secure infrastructure; identity and access control; protecting information; and auditing and reporting.

- Microsoft supports legislation for notification of data breaches that includes a risk-based trigger of notification when data containing personal information is acquired by an unauthorized person, and when there is a significant risk of fraud or identity theft. Notification should not be required where the potential of harm is nominal. However, the law should require that affected individuals be notified within a reasonable time period unless otherwise directed by a law enforcement agency pursuing an investigation.

BACKGROUND

In recent years, media reports of data breaches at major public and private institutions have captured both headlines and public attention, especially when they jeopardized the sensitive personal or financial information of millions. Data breaches not only put consumers at risk of fraud and identity theft, but also threaten their trust of reputable organizations and governments.

Governments at all levels are examining the need to revise data breach notification laws. Current laws typically require companies or agencies to notify customers when their personal data has been put at risk or compromised, and take one of two forms: an acquisition-based trigger or a risk-based trigger.

Acquisition-based triggers require organizations to notify affected individuals when personal information has, or can reasonably be assumed to have been, acquired by an unauthorized person. In contrast, risk-based triggers require organizations to notify affected individuals when a significant potential risk has been identified.

As policymakers develop new policies governing the notification of data breaches, it is worth noting that in some jurisdictions, organizations are exempt from certain disclosure requirements if their data is encrypted at the time of a security breach. This exemption is a powerful motivator for companies to adopt encryption methods and procedures for protecting sensitive data. In addition, 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.

MICROSOFT APPROACH

Microsoft recommends a multifaceted approach to data governance that includes policy, people, processes, and technology. Its approach relies on:

- Strengthened infrastructure with safeguards that help protect systems from malware, intrusions, and unauthorized access to personal information.
- 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.
- Securing sensitive personal information in structured databases and providing safeguards such as encryption for unstructured documents, messages, and records.
- Auditing and reporting on the integrity of systems and data in compliance with business policies.

POLICY CONSIDERATIONS

- Conflicting laws can complicate compliance across local, state, provincial, or national borders. The wide variance in rules, regulations, and laws threatens 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 need to collaborate to develop a mutually agreeable solution that protects both privacy and innovation.
- Microsoft supports data breach notification laws that include:
  - » A risk-based trigger of notification when an unauthorized person acquires data, but only when there is a significant risk of fraud or identity theft.
  - » No requirement of notification when the potential harm to the data subject is nominal, such as where information is encrypted or otherwise unintelligible.
  - » A requirement to notify those affected within a reasonable time period, unless otherwise directed by law enforcement pursuing an investigation.
- While Microsoft supports requirements of mandatory notification when data breaches occur, these requirements should be calibrated to provide timely, meaningful information to consumers. Notification mandates with very short time frames run the risk of giving consumers inaccurate or incomplete information. Broad notification requirements that include all data breaches, even where the risk of harm is negligible, run the risk of flooding consumers with notices that will be ignored.

Helpful Resources

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

February 2013

Microsoft Computing Safety Index

Key Points

- The Microsoft Computing Safety Index (MCSI) is a tool developed as the result of a multiregional survey to determine the best methods for effectively managing and overcoming threats to security and safety online.
- Microsoft uses the MCSI in annual research to identify and rate the online security- and safety-related behaviors of people around the world. Microsoft's research, combined with the resulting index, will help lead to safer technologies and programs for better educating web users.
- The Microsoft Safety & Security Center offers education, guidance, and free tools to help people protect themselves online.
- Microsoft welcomes government support in fighting online security risks, and believes that cooperation with authorities is the most effective way to reduce the impact of cyber threats. Microsoft supports a balanced approach to regulation as part of those efforts.

BACKGROUND

As more people connect online, the need for security, safety, and privacy grows, too. Consumers are increasingly concerned about security breaches, fraud, and the collection and use of personal information. Microsoft believes that a better understanding of how people respond to and defend against these threats can help lead to safer technologies and better programs for educating web users.

To that end, the company commissioned a study in 2010 to learn how people protect themselves online. That research laid the foundation for the development of the Microsoft Computing Safety Index (MCSI), which can be used to assess online safety behavior and security tool use. The index rates more than 20 protective steps people can take—the more steps taken, the higher the online safety score, with 100 being the highest rating possible. The index is based on three tiers of safety activity:

- Foundational (30 points) includes steps consumers can take such as ensuring that antivirus software is installed and up to date, and that automatic updates are turned on.
- Technical+ (40 points) includes managing online information, hiding IP addresses, and monitoring privacy settings.
- Behavioral (30 points) includes using strong passwords, visiting reputable sites, and staying informed about late-breaking security and safety issues.

Microsoft commissions annual research using the MCSI to study how consumers protect themselves and their families online. The 2012 study, which surveyed more than 10,000 adults from 20 countries found that more than half (55 percent) of the respondents are experiencing multiple online risks, yet only 16 percent say they take proactive steps to help protect themselves and their data.

The 2012 survey examined safety behaviors on mobile devices. Researchers found that while 42 percent of those surveyed run software updates on their personal computers, only 28 percent run regular updates on their mobile devices. Other important findings of the 2012 MCSI research:

- The two most common computer threats that respondents experienced were fraudulent email messages asking for personal information or announcing the detection of a virus, and actual instances of viruses, bots, adware, or spyware on their computers.
- Of the respondents, 31 percent had installed mobile antivirus programs on their devices and keep them current; 23 percent reviewed their location and privacy settings when using social media.
- Citizens of Singapore (average MCSI score 42), Malaysia (40), Canada (39), and Australia (39) had the highest scores for online safety on a computer.

MICROSOFT APPROACH

Education and guidance. The Microsoft Safety & Security Center offers online safety guidance to consumers. This includes tips for safer social networking, the use of mobile devices, and responsible online gaming, as well as guidelines for avoiding, blocking, and reporting inappropriate behavior.

Technology tools. Microsoft offers many free technology tools to reduce online risk, including Microsoft Security Essentials, a free antimalware program. In addition, Microsoft has built family safety features into many of its products, including Microsoft Family Safety in Windows 8, which helps monitor and protect children online, and Console Safety Settings for Xbox and Xbox 360.

Security response. The Microsoft Security Response Center employs some of the world's top computer security experts to help Microsoft customers prioritize and manage their responses to cyber threats. When a new threat emerges, the Center's researchers analyze the threat and release security updates to address it.

Policy leadership and collaboration. Microsoft believes that a holistic approach to creating safer online environments requires partnerships with consumers, technology providers, industry, governments, and non-governmental organizations.

POLICY CONSIDERATIONS

- Microsoft believes that cooperation between government and technology industry leaders is the most effective means of reducing cyber threats, and supports balanced regulation as part of that effort. Microsoft believes less onerous industry restrictions will lead to greater innovation and flexibility in responding to cyber crime.
- Microsoft believes in the necessity of working with law enforcement and providing technical training and new technologies to help reduce the impact of cyber crime.
- To improve the overall security of online systems, Microsoft supports government funding for basic security research and welcomes government support for combating cyber threats.
- Microsoft is committed to helping protect consumers by bringing legal action or assisting consumers in their own actions to stop cyber criminals.

Helpful Resources

An abbreviated version of the MCSI survey
aka.ms/MCSISurvey

Microsoft Security Essentials, a free security tool
www.microsoft.com/security_essentials

Microsoft Safety & Security Center
www.microsoft.com/security

February 2013

End to End Trust

Key Points

- End to End Trust is a vision for enabling safer, more trusted computing experiences through broad industry and government collaboration.
- The core concepts of End to End Trust include embracing security and privacy fundamentals; building a trusted stack that spans hardware, software, data, and people; aligning technical, social, political, and economic forces; and creating a claims-based identity meta-system.
- Microsoft is currently working with policymakers, industry partners, and advocates on several important initiatives that include increasing the level of assurance of identity information through in-person proofing, discovering ways to assess the health of devices to help reduce risk, enabling policy-based access control to help protect data as it moves around the Internet, and developing appropriate privacy protections to help users control the disclosure of their data.

BACKGROUND

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

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.

The core concepts of End to End Trust are these:

- **Security and privacy fundamentals**. A trusted online environment relies on technology built from the ground up with security and privacy in mind.
- **Technology innovations**. End to End trust requires an environment in which reasonable and effective trust decisions can be made. This environment depends on a trusted stack—security built into the hardware, trusted software, trusted data, and trusted people.
- **Social, economic, political, and IT alignment**. Technical solutions to implement the End to End Trust vision may fail if there aren't suitable economic models to support them. Solutions could also trigger a backlash if they fail to take into account existing social norms such as privacy. Working together to align technical, economic, political, and social forces greatly increases the ability to make progress.

Microsoft is currently engaged in three key projects with government and industry partners to realize this vision:

- **Verified identity**. High-value transactions, such as online banking, demand a high level of assurance. One way to increase the level of assurance of identity information is to perform in-person proofing. Because many online transactions do not need high levels of assurance, establishing an online identity system that can provide a range of assurance levels is essential. It is also important to build in privacy protections—for example, it may not be necessary to know a person's name. Such a system would support new identity services that would verify claims about people and devices. Microsoft is helping others create such a claims-based identity system.

- **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 the device health project is to create a standards-based solution to verify computing devices that are used for high value transactions.

- **Policy-based data protection**. One of the biggest challenges on the Internet (and in the cloud) is ensuring that sensitive data can be accessed only by those who are authorized to do so. Sensitive data is often shared outside organizations as well as on a wide variety of devices. This project centers on creating solutions that strongly tie data and its access policy together so that no matter where the data ends up, the policy will be honored.

MICROSOFT APPROACH

Microsoft has published the following guidance to help further security and privacy fundamentals:

- The Security Development Lifecycle is a security-assurance process that has been shown to reduce the number and severity of vulnerabilities in software.
- Privacy Guidelines for Developing Software Products and Services offers best practices for developers.

Microsoft technology innovations enhance security:

- Microsoft Security Essentials is a free consumer antimalware solution for Windows XP SP2, Windows Vista, Windows 7, Windows 8, and Windows RT.

- Microsoft Forefront is an integrated portfolio of protection, identity, and access products for organizations both on premises and in the cloud.

- The Microsoft identity and access solution allows organizations to establish and easily maintain a single, consistent representation of identity across the datacenter and cloud. The Information Protection solution automatically discovers, protects, and manages confidential information throughout an organization by integrating with existing platforms and apps.

POLICY CONSIDERATIONS

- Microsoft continues to engage with governments as a trusted advisor, to enhance the security, privacy, and reliability of the cyber ecosystem, and to defend against cyber threats. The company believes that collaboration within industry and with governments through strategic partnerships and outcome-focused initiatives are critical to that mission.

- 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 online crime.

- Microsoft supports government funding of basic security research to help improve the security of online systems.

Helpful Resources

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

Security Development Lifecycle
www.microsoft.com/SDL

Privacy Guidelines for Developing Software Products
aka.ms/privacy-guidelines

February 2013

Microsoft Security Development Lifecycle

Key Points

- The Microsoft Security Development Lifecycle (SDL) is Microsoft's security assurance process for software development that builds security into every phase of software development and provides defense-in-depth guidance and protection.
- The SDL is a hands-on set of procedures involving testers, developers, program managers, and architects working in concert with product security teams across the company. Its security innovations are integrated into Microsoft Office, the Windows operating system, Microsoft SQL Server, and many other Microsoft products and services.
- The SDL is continuously evolving and improving. It is updated to take advantage of newly developed defensive techniques in security science and in anticipation of emerging threats.
- Microsoft shares the SDL with the software industry. The SDL has been adopted (sometimes in a modified form) by a variety of software and hardware vendors, government agencies, and software development organizations.

BACKGROUND

Today's cyber security threats are complex, sophisticated, and ever-changing. They require an ongoing, multifaceted response from the information technology industry for development solutions that optimize software security and provide for safer computing experiences for people around the world.

The Microsoft Security Development Lifecycle (SDL) is Microsoft's security assurance process for software development that introduces security and privacy at every step of the way. It offers a holistic and practical approach to addressing evolving security threats and increasingly sophisticated cyber crime.

Microsoft developed the SDL process in 2004 as part of a defense-in-depth approach to security. It was created to reduce the number of vulnerabilities in Microsoft software and to give users high-quality, meticulously engineered, rigorously tested software that better defends against malicious attacks. Microsoft engineers and security experts realized that performing security activities as part of a repeatable process results in greater security gains and return on investment, and creates a more secure Internet environment. Using the SDL helps developers create software that has fewer, less severe vulnerabilities.

MICROSOFT APPROACH

- Using the SDL is a mandatory practice for product development at Microsoft. As shown below, it comprises a series of systematic security- and privacy-focused activities throughout the software development lifecycle— from technical training for engineers to processes for emergency responses after deployment.

- Software development is an evolving process and so is the SDL. While it's impossible to completely prevent all vulnerabilities during software development, when they do emerge, Microsoft engineers perform root-cause analysis to understand the problem. They then identify corrective actions and incorporate that knowledge into the next version of the SDL.

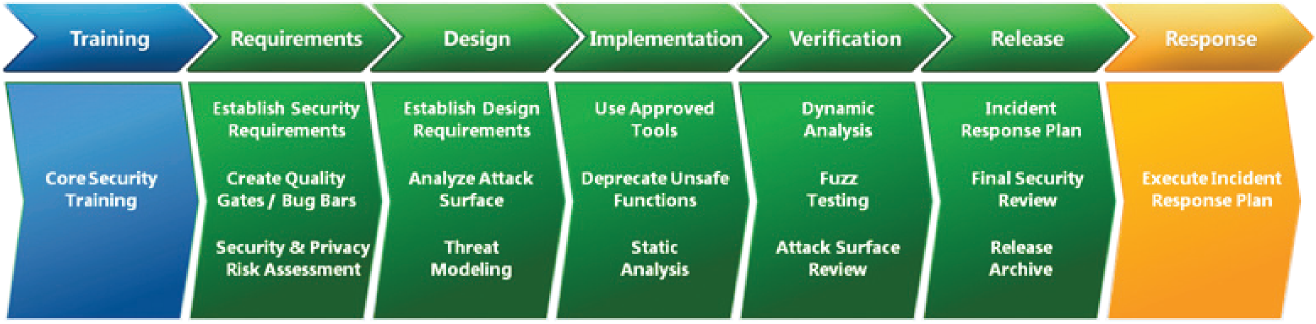
- Implementing the SDL has led to measurable improvements in the security and privacy of Microsoft's products.

POLICY CONSIDERATIONS

- Microsoft believes in a collective approach to security that involves the entire IT community, so the company shares security expertise, process guidance, and technology with developer and IT professional communities worldwide. As of 2012, IT professionals have downloaded Microsoft SDL guidance, white papers, and tools and resources more than a million times.

  The SDL Chronicles document how the Microsoft Security Development Lifecycle has helped public and private organizations change their engineering cultures and develop more secure software. Key industry leaders including Cisco and Adobe have based their security development methods on the Microsoft SDL.

- Any government approach to addressing the problems of information security should also protect innovation and ensure the continued adoption of new technologies. Government and industry can work together to establish appropriate principles that strike the right balance between regulation and innovation.



Helpful Resources

The Security Development Lifecycle
www.microsoft.com/sdl

The SDL Chronicles
aka.ms/SDL-Chronicles

Microsoft Trustworthy Computing
www.microsoft.com/twc/

February 2013

Microsoft Security Intelligence Report

Key Points

- The Microsoft Security Intelligence Report offers a comprehensive, up-to-date, and geographically relevant analysis of the cyber threat landscape of exploits, vulnerabilities, and malware using data from Internet services and over 600 million computers worldwide.
- Microsoft's Trustworthy Computing group is responsible for implementing a long-term, collaborative effort to create and deliver more secure, private, and reliable computing experiences through the Security Science initiative, critical infrastructure protection, delivery of secure products, and defense against malware.
- Microsoft believes that industry cooperation with authorities is the most effective means of reducing cyber threats, and supports balanced regulation as part of that effort.

BACKGROUND

The Internet has become an integral part of everyday life, and as the number of people online grows, so too have concerns about their safety. With good reason: increases in Internet traffic have resulted in dramatic increases in online crime, which has heightened the security concerns of governments and organizations around the world.

Online threats have evolved from petty crimes by attention-seeking hackers to multi-front attacks by sophisticated criminal organizations. Cyber criminals exploit users through email, web browsers, social media, online games, and fake security software. Compromised computers can be used to breach security systems and the data of financial institutions, target political organizations for attacks, and steal people's money or identity—and their sense of security.

As a partner in the global response to online crime, Microsoft provides resources and expertise, including its semi-annual Security Intelligence Report (SIR), to help discover the latest threats. The report offers a comprehensive, up-to-date, and geographically relevant analysis of the cyber threat landscape of exploits, vulnerabilities, and malware using data from more than 600 million computers worldwide and some of the busiest online services on the Internet. The latest SIR, Volume 13: January–June 2012,[1] is over 900 pages of data and analysis with views of 105 countries and regions around the world.

Recent editions of the SIR have shown that cybercriminals are gravitating toward the use of fake software activation keys that contain malware. This emerging social engineering tactic is the number one threat facing consumers worldwide. The SIR also shows that social engineering and similar attacks can be mitigated through security best practices such as implementing effective technical safeguards.

Microsoft appreciates the scope and changing complexities of online security—and the tremendous value of collaborative effort in the event of an attack to provide support, guidance, and the latest information. To that end, the company continues to promote the global imperative of sharing knowledge with industry leaders, governments, and security organizations.

[1] **aka.ms/SIR-V13**

MICROSOFT APPROACH

The Trustworthy Computing group at Microsoft is responsible for implementing a long-term, collaborative effort to create and deliver more secure, private, and reliable computing experiences. Areas of the group's focus include:

- **Security Science.** Building on a body of research about how systems are attacked and ways to prevent or mitigate those attacks, Security Science is a Microsoft initiative that develops tools and techniques to make attacking systems more difficult. Through Security Science, Microsoft continually monitors threat trends and looks for software vulnerabilities. The company then uses that information to create mitigation tools and techniques that developers can draw on to improve overall security.
- **Protection of critical infrastructure.** With technology becoming ever more important in people's daily lives, the Trustworthy Computing team engages with governments around the world to help them protect critical infrastructures as well as the safety of their citizens online. The team is committed to sharing its research and innovations to help establish policies that make meaningful improvements to global cyber security.
- **Delivery of secure products.** The Microsoft Security Engineering Center helps protect Microsoft customers by delivering more secure products through the Microsoft Security Development Lifecycle (SDL). The SDL is the industry-leading software security assurance process, which embeds security and privacy through every phase of the development of Microsoft products.
- **Combating malware.** The Microsoft Malware Protection Center analyzes malicious software and develops solutions that Microsoft uses in its security technologies. When a vulnerability in Microsoft software is discovered, the Microsoft Security Response Center monitors and responds to the incident. It also manages the company's process for releasing security updates, and serves as the single point of coordination.

POLICY CONSIDERATIONS

- Microsoft welcomes the support of governments in fighting online security threats. The company believes that industry cooperation with authorities is the most effective means of reducing cyber threats, and supports balanced regulation as part of that effort. Microsoft believes 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 the Convention on Cybercrime ratified by the Council of Europe, which requires signatories to adopt and update laws and procedures that address online crime.
- Microsoft supports the government funding of basic security research to help improve the security of online systems.

Helpful Resources

Microsoft Security Response Center
www.microsoft.com/msrc

Microsoft Security Intelligence Report
www.microsoft.com/sir

Microsoft Malware Protection Center
www.microsoft.com/mmpc

Convention on Cybercrime
aka.ms/Convention-on-Cybercrime

February 2013

Microsoft Security Response Center

Key Points

- The Microsoft Security Response Center (MSRC) serves as Microsoft's single point of security coordination and communications and is led by some of the world's most experienced experts. The MSRC identifies, monitors, resolves, and responds to security incidents including vulnerabilities in Microsoft software. The MSRC also manages monthly security updates and publishes the Security Update Guide, Security Advisories, and a semi-annual Security Intelligence Report.

- Microsoft encourages reasonable, coordinated disclosure of vulnerabilities in its software and works to mitigate the exploitation of vulnerabilities through MSVR, MAPP, and the Microsoft Exploitability Index.

- 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, including through BlueHat security briefings and ICASI.

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), part of the Trustworthy Computing Group, was created to help keep pace with evolving threats and better protect customers against malicious attacks through timely security updates and authoritative guidance. The MSRC, led by some of the world's most experienced security experts, serves as Microsoft's single point of coordination and communication on security threats.

Each year, the MSRC manages over 100,000 reports of vulnerabilities in Microsoft software. It also draws on a worldwide network of security researchers and partners that closely monitors online security news lists and public forums. The MSRC identifies, monitors, responds to, and resolves security incidents following a four-step process when it receives information about a potential threat.

- **Evaluation**. The team evaluates the possible impact of the threat to customers.
- **Investigation**. MSRC experts gather enough information to reproduce the vulnerability and determine which products or services might be affected.
- **Severity rating**. The MSRC rates each vulnerability according to severity and the likelihood that it will be exploited.
- **Resolution**. The team decides whether to fix the problem with an immediate update to Microsoft software, or to resolve the issue in a future service pack or new product version.

The MSRC is committed to providing timely and prescriptive guidance and communicates with customers through a number of channels including blogs, bulletins, advisories, and webcasts.

- Since 2003, the MSRC has managed the release of software security updates company-wide to address vulnerabilities in Microsoft software. MSRC experts also write the Microsoft Security Bulletin, which is translated into multiple languages and published the second Tuesday of every month.

- In 2005, Microsoft introduced a supplement to these bulletins, Microsoft Security Advisories, which addresses security changes that may not require a bulletin but that may still affect customers' overall security.

- The MSRC developed the Microsoft Security Update Guide to help IT professionals better understand and maximize Microsoft security update release information, processes, and tools.

- The MSRC publishes the semi-annual Microsoft Security Intelligence Report, a comprehensive, up-to-date, and geographically relevant analysis of the cyber threat landscape of exploits, vulnerabilities, and malware. It draws on data from more than 600 million computers worldwide and some of the busiest online services on the Internet.

MICROSOFT APPROACH

Microsoft encourages reasonable, coordinated disclosure of vulnerabilities in its software and works to mitigate exploitation of them.

- **Microsoft Vulnerability Research (MSVR)** is a program through which Microsoft shares its collective experience and best practices in dealing with vulnerabilities within the security community. The goal is to foster positive change, which will ultimately improve the security ecosystem.

- **Microsoft Active Protections Program (MAPP)** offers security software providers information about vulnerabilities from the MSRC in advance of Microsoft's monthly security update. This advance warning gives these MAPP partners more time to build protections against the vulnerability so they can give their customers updated protections faster.

- **The Microsoft Exploitability Index**. In 2008, Microsoft launched the Index to help customers evaluate risk by providing information on the likelihood that a vulnerability addressed in a Microsoft security update will be exploited within the first 30 days of the update's release.

Microsoft collaborates with the security community and with partners to advance and improve security for customers and build a more trusted Internet.

- **BlueHat security briefings** are invitation-only conferences aimed at improving the security of Microsoft products. Microsoft security professionals and outside researchers come together to share ideas, and expertise about threats to global security.

- **Industry Consortium for Advancement of Security on the Internet (ICASI)**, co-founded by Microsoft, is a nonprofit corporation of leading IT companies that addresses international, multi-product security challenges to better protect the IT infrastructures that support the world's enterprises, governments, and citizens.

Helpful Resources

Microsoft Security Response Center
www.microsoft.com/msrc

MSRC blog
blogs.technet.com/msrc

Microsoft Security Intelligence Report
www.microsoft.com/sir

Microsoft Security Update Guide
aka.ms/msrc-guide

Microsoft Vulnerability Research (MSVR)
aka.ms/ms-msvr

Microsoft Active Protections Program (MAPP)
aka.ms/ms-mapp

Industry Consortium for Advancement of Security on the Internet (ICASI)
www.icasi.org

Microsoft Exploitability Index
aka.ms/Exploitability-Index

Microsoft Trustworthy Computing
www.microsoft.com/twc

Supply Chain Security

Key Points

- Governments worldwide have concerns about supply chain security, in particular the potential for hostile actors to insert malicious software into information technology products as they move through the supply chain. This could create vulnerabilities in the information and communications technology systems when compromised components are introduced.

- Microsoft employs a four-part strategy to manage the risks to its products and services in the supply chain. This strategy is grounded in identity and access management controls, the Security Development Lifecycle, policies and procedures that monitor the integrity of Microsoft software, as well as anti-counterfeit measures.

- Governments and businesses need to recognize that supply chain security is a shared problem, and that they must work together using risk-based solutions, best practices, and international cooperation.

BACKGROUND

Information and communications technology systems perform an increasingly important role in commerce and in daily life. Some of the more critical systems have become attractive targets for malicious actors who mount increasingly sophisticated attacks that have the potential to cause widespread damage or disruption, or give them unauthorized access to data.

A key area of criminal interest is the supply chain of technology products, which the National Institute for Standards and Technology defines as “the set of organizations, people, activities, information, and resources for creating and moving a product or service (including its sub-elements) from suppliers through to an organization’s customers.”

The supply chain responsible for delivering information and communications technologies is globally distributed. The products themselves can be complex, made of many parts in many different companies all over the world. This raises concerns about the potential for hostile actors to introduce malicious or unwanted functions or counterfeit elements along the way. If products are compromised, they could potentially be used to conduct surveillance or to disrupt or otherwise degrade the trustworthiness of the information and communications technology systems of which they will be a part.

Securing such a diverse and global supply chain presents a challenge for governments and businesses. Both need to recognize supply chain security as a shared problem and seek solutions that are built upon best practices, mitigate risks, and draw on international cooperation.

MICROSOFT APPROACH

Microsoft's strategy to help mitigate supply chain risk to its products and services includes:

- **Identity and access management controls.** Microsoft uses policies, procedures, and technology that manage personnel access to Microsoft intellectual property.
- **The Security Development Lifecycle** is a foundational element for reducing the risk in the development of Microsoft software, and for protecting it against the introduction of product vulnerabilities, whether malicious or inadvertent.
- **Software integrity controls.** Microsoft employs policies, procedures, and technology to preserve the integrity of its software products, including code signing and checking for malware.
- **Anti-counterfeit measures.** To protect customers from the risks of counterfeit software, which could contain vulnerabilities, Microsoft actively identifies counterfeit versions of its software, works to maintain the integrity of its distribution models, and works closely with law enforcement agencies around the world to help reduce piracy.

Microsoft also takes legal and technical action to address criminal efforts to target the supply chain. For example, the Microsoft Digital Crimes Unit works with other Microsoft teams to fight aggressively against botnets. One such initiative is Project MARS (Microsoft Active Response for Security), which focuses on efforts to disrupt criminal infrastructure. This includes taking legal and technical action to pursue botnets and help undo the damage they cause. In 2012, Project MARS helped take down the Nitol botnet, which infected computers through vulnerabilities in the supply chain.

POLICY CONSIDERATIONS

A framework for managing supply chain risk should rest on these principles:

- **Risk-based approach.** Governments should avoid using simplistic factors such as a product's country of origin to assess risk. The global character of many products means that attempts to prohibit products based upon country of origin could result in a broad ban of products. This would lead to weakening open trade and relinquishing the benefits of global innovation. Instead, governments should rely on tested risk-management principles.
- **Transparency.** Governments have a right to expect IT companies to provide an appropriate degree of visibility into their business processes and the controls that ensure the security of their product development and operations.

  One example of such transparency is Microsoft's Government Security Program, which gives eligible participating governments access to the source code for selected Microsoft products. While expecting transparency, however, governments also need to appreciate that businesses must protect their trade secrets and other intellectual property.
- **Flexibility.** When governments move to adopt standards governing supply chain security, control and mitigation standards need to remain flexible.
- **Reciprocity.** The development of reciprocal international standards for supply chain security is essential for continuing to realize the benefits of the Internet that rely on the security and integrity of information technology systems.

Helpful Resources

Microsoft Global Security Strategy and Diplomacy
www.microsoft.com/gssd

Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust
aka.ms/supply-chain-risk

Toward a Trusted Supply Chain: A Risk Based Approach to Managing Software Integrity
aka.ms/Trusted-Supply-Chain

The Microsoft Security Development Lifecycle
www.microsoft.com/sdl

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

February 2013

Privacy: An Overview

Key Points

- Consumers expect strong privacy protection to be built into their products and services, and have high expectations about how companies collect, use, and store their information. Public trust depends on people knowing that their privacy will be protected and that their personal information will be used appropriately.
- Microsoft has a longstanding commitment to privacy. The company takes steps to responsibly manage customer information, promote transparency, and offer meaningful privacy choices. Microsoft employs more than 40 people who work full-time on privacy, and several hundred other employees worldwide focus on privacy as part of their jobs.
- Microsoft supports privacy legislation that facilitates the free flow of information, builds trust, and encourages innovation. Because data increasingly flows across geopolitical borders, the company favors greater standardization and better worldwide alignment of privacy regulations, policies, and standards.

BACKGROUND

The digital economy has changed the world in profound and exciting ways. At the same time, public concern about privacy, including the collection and use of personal information and widely publicized data breaches, threatens to erode public confidence in digital commerce and the Internet.

Consumers expect strong privacy protection to be built into their products and services, and have high expectations about how companies collect, use, and store their information. Public 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, people may be less inclined to use online technologies, and both industry and people will suffer.

MICROSOFT APPROACH

Microsoft has a longstanding commitment to privacy. The company takes steps to responsibly manage customer information, promote transparency, and offer meaningful privacy choices:

- **Privacy fundamentals.** Microsoft understands that respect for privacy is essential to a computing environment that is trustworthy. Microsoft employs more than 40 full-time privacy professionals and several hundred more employees worldwide who are responsible for ensuring that privacy policies, procedures, and technologies are applied company-wide.
- **Protection of user information.** Microsoft believes that people should have control over their personal information and that organizations should be responsible and accountable for how they collect, use, and protect this information. Microsoft's privacy principles and privacy statements provide clearly worded explanations of what information Microsoft collects (and why), and how Microsoft uses it. They also offer guidance on how individuals can manage some of the information they provide to Microsoft.

- **Policy leadership and collaboration**. Microsoft works with governments, businesses, and technology industry leaders to advise on legislative proposals, help align laws across jurisdictions, develop responsible privacy practices, and strengthen self-regulatory mechanisms that support greater protections for individuals and their personal information.

  The company's public policy efforts include advocating for new and updated regulatory approaches to promoting a safer, more open cloud computing environment, and baseline federal policy legislation. Microsoft also works with law enforcement agencies as well as consumer and advocacy organizations around the world to combat fraud, spam, spyware, and other threats to privacy online.

POLICY CONSIDERATIONS

- Microsoft supports privacy legislation that facilitates the free flow of information, builds trust, and encourages innovation. Because data exchanges are increasingly global, the company favors greater alignment of privacy regulations, policies, and standards worldwide.
- As governments act to address issues associated with emerging technologies and online services, they should not stifle innovation and the adoption of technology in the process. Government and industry can work together to establish appropriate and balanced principles that can be standardized and applied globally.
- Microsoft believes that the way data is used, rather than how it is collected, could be a more effective premise for protecting data and meeting privacy obligations related to that data. Rather than relying on notice and consent, Microsoft supports a model based on use.

Helpful Resources

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

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

Microsoft privacy statement
aka.ms/privacy-statement

Privacy Guidelines for Developing Software Products and Services
aka.ms/privacy-guidelines

Privacy and cloud computing at Microsoft
www.microsoft.com/privacy/cloudcomputing.aspx

Privacy in Microsoft advertising
choice.microsoft.com

February 2013

Baseline Privacy Legislation

Key Points

- In countries that lack comprehensive privacy laws (including the United States), local, state, and federal government policymakers should 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 in the United States since 2005. The company advocates national legislation that will give people greater control over the collection, use, and disclosure of their information and a greater sense of security about their transactions.

- Microsoft believes that baseline privacy legislation should apply to both online and offline computing and should include requirements for transparency, consumer control, and security. Privacy legislation should create legal certainty by preempting local laws that are inconsistent with national policy. It should also promote accountability by ensuring that all businesses are using, storing, and sharing commercial data in responsible ways.

- Privacy legislation cannot be expected to solve all these challenges. To achieve the broadest protection for consumers, such legislation should be paired with industry self-regulation and best practices, technology solutions, and consumer education.

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 some countries that lack such comprehensive national laws (including the United States), privacy is governed through a combination of local 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.

Baseline national privacy legislation would help create legal certainty by preempting state or provincial laws that are inconsistent with national policy. It could promote both accountability and innovation by helping to ensure 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.

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. Greater clarity and alignment of regulatory efforts can improve transparency, security, and consistency—and give consumers greater control over their personal information.

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

MICROSOFT APPROACH

- Microsoft has been a leading advocate for comprehensive federal privacy legislation in the United States since 2005. The company believes that federal legislation is necessary to give consumers greater predictability regarding the collection, use, and disclosure of personal information and greater confidence in their online and offline transactions.

- Microsoft's longstanding commitment to privacy includes principles, policies, and procedures for building privacy protections into its products and services—from development through deployment and operation.

- Microsoft shares information and ideas about many of the privacy-related legislative proposals that are taking shape around the world. The company's efforts include providing comments and feedback to the U.S. Federal Trade Commission (FTC) on the preliminary staff report on consumer privacy and on supplemental proposed revisions to the rule implementing the Children's Online Privacy Protection Act (COPPA). Microsoft also participated in the consultation process for the European Union Data Protection Directive, and supported the development of the Asia-Pacific Economic Cooperation Privacy Framework.

POLICY CONSIDERATIONS

- Microsoft believes that baseline privacy legislation should apply both online and offline, and should include requirements for transparency, consumer control, and security. Legislation should create legal certainty by preempting state or provincial laws that are inconsistent with federal policy. It should also promote accountability by ensuring that all businesses use, store, and share data responsibly, while encouraging competition on the basis of more robust privacy practices.

- Privacy 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 to protecting consumer privacy will be to pair baseline legislation 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 therefore better address and adapt to emerging technologies and rapidly evolving business models.

Helpful Resources

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

Privacy and cloud computing at Microsoft
www.microsoft.com/privacy/cloudcomputing.aspx

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

February 2013

International Data Protection Standards

Key Points

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

BACKGROUND

The Internet and cloud computing are erasing geographic boundaries for the flow of information. 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. This international flow of information benefits the global economy: it delivers new efficiencies, opens up new markets, and creates tremendous opportunity.

Yet when data is shared across regions, it's not always clear which laws, regulations, and protection principles apply. Today's regulatory models are based on a way of doing business that existed before digital globalization. In the European Union, for example, 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 industry—for example, different privacy laws apply to healthcare and finance. For companies that conduct international business, such complex compliance requirements add to the cost of doing business.

Industry should work with government to develop more consistent frameworks that streamline the 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 in 2010 passed a resolution that called for the organization of an intergovernmental conference with the goal of developing a binding international instrument on personal data protection and privacy. Also, the International Standards Organization (ISO) continues to develop consistent and predictable standards that help to protect data security and privacy around the world.

MICROSOFT APPROACH

Microsoft's longstanding commitment to privacy includes principles, policies, and procedures for building privacy protections into its products and services, from development through deployment and operation.

- Microsoft's privacy standards govern the development and deployment of Microsoft products and services. These standards, a version of which have been made public, offer detailed guidance on customer notification and consent procedures, help make sure data security features are sufficient, maintain data integrity, and provide user access and controls. Microsoft also helps to protect customers by delivering more secure products through the Microsoft Security Development Lifecycle (SDL), a software security assurance process which embeds security and privacy throughout product development. Microsoft designs its cloud services to help ensure data security and user privacy.

- Microsoft works to help ensure that employees, vendors, and partners are accountable for the handling of customers' personal information. 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 monitoring and protecting privacy.

- Microsoft follows and implements international privacy and data protection standards. For example, Office 365 is compliant with ISO 27001.

POLICY CONSIDERATIONS

- Microsoft supports current efforts to harmonize data protection rules and is a strong proponent of extending the ISO 27001 standard and its data protection controls as the basis of those rules. Broadly adopted and consistently applied, ISO standards can help to support the protection of cloud-based data.

- International privacy standards should be flexible and technology-neutral, and should be applied across sectors.

- Microsoft supports an accountability-based approach to data privacy, which permits data to be transferred across international borders without restrictions as long as the data exporter remains accountable for protecting the data regardless of its geographic location. This approach would hold organizations responsible for protecting data while still giving them flexibility to accommodate evolving data transfer needs.

- In order to optimize the efficiency of online services and deliver the 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

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

Privacy and cloud computing at Microsoft
www.microsoft.com/privacy/cloudcomputing.aspx

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

February 2013

Location-Based Services and Privacy

Key Points

- Location-based services offer many useful apps, such as real-time maps and the ability to locate local businesses, but customers will not fully adopt the services unless proper privacy safeguards are in place.
- Microsoft's privacy standards govern the development and deployment of its location-based services and apps. These include procedures for customer notification and consent, data security, and privacy controls.
- Microsoft believes that the information and communications industry should work with civil society, governments, and others to create appropriate guidance for protecting the privacy of personal location data.

BACKGROUND

Location-based services give customers information based on their geographic location. They offer real-time navigation software, social networks that allow customers to check in as they go from place to place, local weather, geographically targeted search engine results, and other useful functions. The geolocation data is gathered in a number of ways—through global positioning system (GPS) technology built into devices, IP addresses, or Wi-Fi network mapping.

A 2010 survey[1] conducted for Microsoft in the United Kingdom, Germany, Japan, the United States, and Canada found that 94 percent of customers who had used location-based services considered them valuable. However, the same survey found that 52 percent were concerned about the potential for loss of their privacy through the use of geolocation data.

Among the privacy concerns related to location-based services:

- **Notice.** Customers want to receive adequate notice that an app will collect and use their geolocation data and give their consent for it to do so.
- **Control.** Customers want to have access to and be able to limit the collection and use of their data.
- **Retention.** Customers want to be informed about the policies that govern the retention of their data.
- **Reuse.** Customers want to choose how their data will be used and how it might be combined with other data.
- **Disclosure to third parties.** Customers want to control how their data is shared with third-party apps.
- **Court orders.** Customers want to be know if their geolocation data might be requested and released by court order.

[1] *Location-Based Services: Usage and Perceptions*
aka.ms/Location-Research

MICROSOFT APPROACH

Microsoft is involved in many aspects of providing LBS, including as a provider of apps and as an operating system platform for third-party apps, both of which use LBS.

- Microsoft applications that use location-based products and services undergo a privacy review designed to identify issues and help product teams follow Microsoft privacy policies and standards.
- Windows Phone applications that use location are contractually required to provide the ability to turn off that application's access to an individual's location.
- Users can control a number of features that impact their privacy by using the **Express Settings** or **Customize** options. These may include features that may share information with apps, such as a single setting to manage access to the Windows Location Platform.

  If the platform is turned on when a user runs a Windows Store app for the first time, Windows will ask the user whether the app may access the user's location. Conversely, if the platform is turned off, apps cannot use the Windows Location Platform to access the user's location. At any time while using a Windows Store app, the user may easily enable or disable use of location.

POLICY CONSIDERATIONS

- Microsoft has a longstanding commitment to privacy legislation initiatives that facilitate the free flow of information, build trust, and encourage innovation.
- As governments address issues associated with emerging technologies and online services, it is important that they not stifle innovation and technology adoption in the process.

Helpful Resources

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

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

Bing Maps privacy questions and answers
www.microsoft.com/maps/streetside.aspx

Windows 8 app certification requirements
aka.ms/app-cert

Windows Phone Privacy Resources
aka.ms/WindowsPhone-Privacy

February 2013

Microsoft Privacy Statements

Key Points

- Improvements to Microsoft online privacy statements enhance their design and functionality to more effectively layer important information and make that information easier to locate and use.
- Migration to the new format will be gradual but steady. Bing and Microsoft.com were the first to adopt it, followed by Xbox; other Microsoft products and services will follow over time.
- Microsoft remains steadfast in its longstanding commitment to protecting customer data, and continues to stand behind its privacy policies and practices. There are no material changes to Microsoft's data collection and use practices as a result of the redesign.

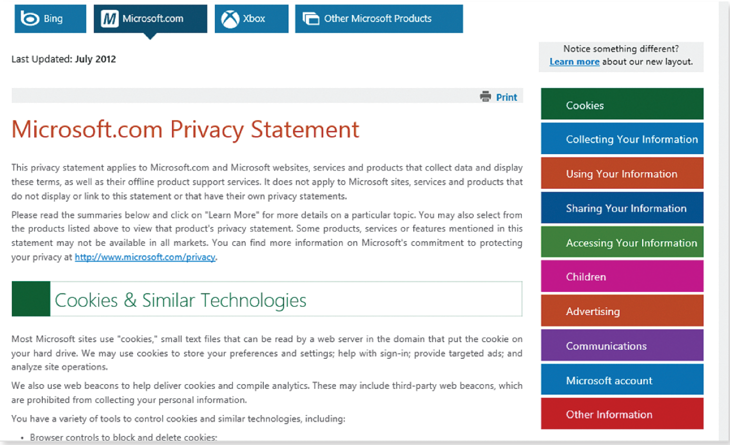
BACKGROUND

Privacy statements describe the information a company collects and how that information is used and shared. However, the increasingly complex nature of global data flows, along with new privacy regulations, has led to privacy statements that are often lengthy and difficult to read. In addition, many organizations have dozens (even hundreds) of different online resources or services, which can lead to multiple, overlapping privacy statements.

The challenge for companies is to create privacy statements that convey the most important elements in a clear and understandable way, and offer easy access to additional details for those seeking more complete information.

One way to accomplish these goals is through a layered privacy notice. A layered privacy notice lists the most important features of the privacy policy, such as what information is collected and how it is used. After each feature, viewers are offered a link to more detail. In 2006, Microsoft was one of the first companies to implement a layered privacy statement.

In July 2012, Microsoft updated its online privacy statements to enhance their functionality and provide greater consistency across Microsoft products and services. Migration to the new format is ongoing with Bing and Microsoft.com (illustrated below) the first to adopt the new format, followed by Xbox in October 2012.



Last Updated: **July 2012**

Notice something different?
Learn more about our new layout.

Microsoft.com Privacy Statement

This privacy statement applies to Microsoft.com and Microsoft websites, services and products that collect data and display these terms, as well as their offline product support services. It does not apply to Microsoft sites, services and products that do not display or link to this statement or that have their own privacy statements.

Please read the summaries below and click on "Learn More" for more details on a particular topic. You may also select from the products listed above to view that product's privacy statement. Some products, services or features mentioned in this statement may not be available in all markets. You can find more information on Microsoft's commitment to protecting your privacy at http://www.microsoft.com/privacy.

Cookies & Similar Technologies

Most Microsoft sites use "cookies," small text files that can be read by a web server in the domain that put the cookie on your hard drive. We may use cookies to store your preferences and settings; help with sign-in; provide targeted ads; and analyze site operations.

We also use web beacons to help deliver cookies and compile analytics. These may include third-party web beacons, which are prohibited from collecting your personal information.

You have a variety of tools to control cookies and similar technologies, including:

- Browser controls to block and delete cookies;

MICROSOFT APPROACH

The new format and design of Microsoft's privacy statements:

- Enhance their functionality by enabling more effective layering of important information and creating a consistently accessible structure across many Microsoft products.
- Make it easier and more efficient for customers to discover and go directly to the privacy statement for the specific product or service they are using.
- Include clearly defined subsections specific to different types of data collection and use such as advertising and cookies, how information is collected and used and why it's shared, how users can access their information, and privacy, especially as it applies to children.

Microsoft remains steadfast in its longstanding commitment to protect customer data, and continues to stand behind its privacy policies and practices. There are no material changes to Microsoft's data collection and use practices as result of this redesign.

POLICY CONSIDERATIONS

- Governments and industry alike have a vested interest in ensuring that privacy notices are transparent, discoverable, and easy to understand. To that end, Microsoft believes that flexible legislative frameworks will help to ensure both that consumers have robust privacy protections, and that businesses are able to develop and offer innovative products and services. Legislation that follows these criteria will also be more resilient to technological and business change, helping to protect consumer data not only today, but in the years to come.
- While governments have an important role in encouraging companies to provide clear and understandable privacy statements for consumers, they should avoid mandates that could lead to "one size fits all" privacy policies.
- People's privacy expectations vary depending on the nature of their relationship with a specific company. Any legislation, therefore, should permit businesses to adapt their policies and practices to the context in which personal information is used and shared.

Helpful Resources

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

Microsoft's Privacy Statement
www.microsoft.com/privacystatement

February 2013

Next-Generation Privacy Models

Key Points

- The current data protection model of notice and consent as the primary means for individual control should be reconsidered, in light of the burden to consumers posed by the increasingly complex uses and reuses of their data.
- Instead, other models of control should be considered, such as a model based on the use of data. This may be more appropriate for the privacy protection of both the organizations that collect data from individuals and other parties that may also use data.
- A model based on use can exist with many current fair information practices, as well as applicable law, and in no way diminishes the requirement that information be collected in a fair and lawful manner.

BACKGROUND

In January 2002, Bill Gates sent an email to all Microsoft employees announcing the Trustworthy Computing Initiative. His email outlined what today are still the key tenets of trustworthy computing: security, privacy, and reliability. Gates recognized that privacy concerns would be critical to building trust in information technology and, as a result, Microsoft invested heavily in a privacy program. These investments continue to help foster opportunities for its engineers to create technologies, services, and features that are based on customer needs, including sensitivity to their privacy concerns.

Traditionally, data privacy in many parts of the world has been based upon the concept of Fair Information Practices, which include notions such as notice and consent. These require a company to give notice to individuals 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 inconsistent with the consumer's choice. Consumers give their consent by agreeing to the privacy statement. In some jurisdictions, consent requirements play an even larger foundational role in privacy protection models.

In the modern information economy, however, the massive aggregation of computer data (sometimes referred to as big data) and cloud computing are creating highly complicated flows of data, putting the notice-and-consent model under heavy strain in three significant ways:

- First, choices regarding collection of an individual's data and its use have become so complex they are difficult for most individuals to understand, let alone manage.
- Second, the model assumes an interactive relationship between the individual and the entity collecting and using the data, a relationship that increasingly may not actually exist.
- Third, the true value of data may not be understood at the time of collection, and future uses that have significant individual and societal benefit may be lost if privacy models focus solely on the collection of data.

Asking individuals to assume responsibility for policing the use of data in this environment is no longer reasonable, nor does it offer sufficient checks against inappropriate and irresponsible data use. As a result, consumers have a disproportionate burden of responsibility.

Instead, a model based on the use of data may be better suited as a means of providing effective protection for both the organizations that collect data from individuals and parties that use it. Such a use model requires all organizations to be transparent, offer and honor appropriate choices, and ensure that risks to individuals related to data use are assessed and managed. Such an approach also emphasizes the need for greater accountability by organizations that manage and share personal data.

A model based on use would be designed to help achieve five goals: (1) protect privacy in meaningful ways; (2) optimize the use of data for the benefit of both individuals and society; (3) ensure that those who use data are accountable for its use; (4) provide a regime that permits more effective oversight by regulators; and (5) work effectively in a modern connected society. In a data-rich world, achieving these objectives requires meaningful user control and transparency.

MICROSOFT APPROACH

- Microsoft believes that the way data is used, rather than how it is collected, could be a more effective premise for defining data protection and privacy obligations related to that data. Microsoft supports an approach that emphasizes a model based on use rather than relying on traditional notice and consent.
- Microsoft recognizes the need for self-regulatory principles governing data usage that give individuals greater control over their data and greater transparency into how companies manage and use their data. Microsoft's own practices include commitments to customer notice of and control over data use, and to providing data security.
- Microsoft's privacy principles are generally tailored to account for the types of information the company collects and how it intends to use that information.

POLICY CONSIDERATIONS

- Microsoft encourages the adoption of privacy models based on use within self-regulatory principles, a concept being explored in legislative proposals in both the United States and Europe.
- A model based on use can exist with current fair information practices, as well as applicable law, and in no way diminishes 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.

Helpful Resources

Microsoft Trustworthy Computing Next
www.microsoft.com/twcnext

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

A Use and Obligations Approach to Protecting Privacy: A Discussion Document. The Business Forum for Consumer Privacy, December 2009.
aka.ms/Use-Discussion

February 2013

Privacy Accountability

Key Points

- Under the principle of accountability for data privacy, 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 personal data.

- Accountability for data privacy is a key Microsoft principle that helps determine how the company and its vendors and partners manage personal information. Each Microsoft business unit is responsible for developing procedures to uphold the company's commitment to protecting personal data.

- Microsoft supports an accountability-based approach to public policy, which permits data to be transferred across international borders without restriction as long as the data exporter remains accountable for protecting the data regardless of its geographic location.

BACKGROUND

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

Accountability is best defined as an approach that requires companies that process and store data to analyze and understand the privacy risks this raises for individuals, and take necessary and appropriate steps to mitigate those risks. They must implement programs that align with data protection principles, take responsibility for the safe and appropriate processing and storage of data regardless of its location, and be able to explain how their programs provide the required protections for individuals' data.

The importance of accountability for data protection and privacy has never been greater. Technical innovations related to data collection, analysis, and processing, greater access and flow of data worldwide, and the development of powerful analytic tools have created a situation where more potentially usable data about more people exists than ever before. This new world of accessible, interconnected data requires meaningful privacy safeguards.

Accountability for data privacy has experienced a recent resurgence in privacy policy circles worldwide, with a number of countries developing privacy frameworks that include accountability.

The widespread adoption of a principle of accountability offers many potential benefits. It facilitates the flow of data across international borders, and enables cloud computing by requiring that businesses take responsibility for the management of information regardless of where it resides or is processed.

MICROSOFT APPROACH

- A key Microsoft privacy principle is that of accountability in handling its customers' personal information within the company and with its vendors and partners.
- Each Microsoft business unit is accountable for developing procedures to safeguard data and for assigning specific staff members responsibilities for privacy protection, enforcement, and monitoring.
- Microsoft works with policymakers and other stakeholders to consider how the accountability model might work, how organizations can advance accountability, and what role third-party accountability agents and other validation programs might play in this evolving paradigm.

POLICY CONSIDERATIONS

- Microsoft supports public policies that take an accountability-based approach to data privacy, which permits data to be transferred across international borders without restriction as long as the data exporter remains accountable for protecting the data regardless of where it resides or is processed. This approach holds organizations responsible for protecting data, while still giving them flexibility to accommodate evolving data-transfer needs.
- Microsoft believes that policymakers and other stakeholders should carefully consider how the accountability model might work within legal regimes so as to better protect consumers—while minimizing burdens on organizations and providing clear benefits to those that demonstrate responsible data protection practices, such as through the facilitation of trans-border data flows.
- Microsoft does not believe that regulators should use accountability to impose burdensome external validation mechanisms. For instance, third-party audits or certification schemes can be onerous, expensive, and disproportionate to the potential privacy risks.

Helpful Resources

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

The Role and Importance of Organizational Accountability in Managing and Protecting Users' Data
aka.ms/accountability-privacy

A collection of accountability-related papers from the Information Policy Centre
aka.ms/accountability-papers

February 2013

Privacy by Default

Key Points

- Microsoft recognizes the important role that default settings can play in protecting privacy; however, a prescriptive approach to Privacy by Default could lead to unintended consequences, such as limited innovation, limited functionality, and user frustration.
- Microsoft believes that the goals of Privacy by Default are best accomplished when default settings are tailored to the technology or service. Appropriate default settings are best determined on a case-by-case basis as part of an overall approach to implementing Privacy by Design.
- Microsoft products and services undergo privacy reviews, which identify privacy issues and help product teams follow Microsoft privacy policies and standards.

BACKGROUND

Privacy settings play an important role in helping people protect their privacy online. Consumers expect companies to create privacy settings that provide transparency and control over the ways that organizations collect, use, and store personal information. Companies with online operations and services must develop privacy practices that meet these expectations.

Privacy by Default is a software design concept that is presently being considered by a number of data protection authorities, including the European Commission. Broadly defined, Privacy by Default would prohibit the collection, display, or sharing of any personal data without explicit consent from the customer. More detailed definitions often include a requirement that privacy settings that limit the sharing of personal data be turned on by default. For example, a social networking service would not make any information about customers publicly viewable until customers take affirmative steps to allow it.

Advocates for Privacy by Default claim that many people don’t know how to actively enable their privacy settings; that people believe it’s too difficult or tedious to configure privacy settings; or that a lack of default settings can lead to a higher risk to children’s privacy on services such as social networks.

There are a number of challenges to implementing Privacy by Default. First, it’s problematic to create universally agreed-upon settings that address all types of software and online resources. It’s also difficult to create and implement settings that satisfy the needs of a broad range of customers. Finally, Privacy by Default could result in software design that confuses and frustrates customers with repeated notices and warnings.

MICROSOFT APPROACH

- **Privacy by Design at Microsoft** describes not only how Microsoft builds products, but how the company operates its services and organizes itself as an accountable technology leader. For Microsoft, it includes all of the people, processes, and technologies that help maintain and enhance privacy protections. Privacy by Design is in place because the company must earn the trust of customers and partners every day by being as transparent as possible about those policies and processes.

- **Accountability** for data privacy is a key Microsoft principle that determines how the company and its vendors and partners manage the personal information of Microsoft customers. Each Microsoft business unit is responsible for developing procedures to uphold the company's accountability commitment.

- **Case-by-case approach.** Microsoft believes the goals of Privacy by Default are best accomplished when the default settings are appropriate to the context of the technology or service and are determined on a case-by-case basis.

- **Education.** Microsoft knows customers want and expect strong privacy protections built into its products and services, and is committed to providing tools to assist people in making better choices about their online privacy. To help people better manage their personal information online, Microsoft created a Privacy in Action page that explains Microsoft privacy settings, offers videos about how people can protect their privacy online, and includes a report on Microsoft's privacy research.

POLICY CONSIDERATIONS

Microsoft believes privacy regulations should meet certain fundamental requirements:

- **Technology neutrality.** There is no question that technology will continue its rapid change. Consequently, any privacy regulation framework should avoid preferences for specific services, solutions, or mechanisms to provide notice, obtain choice, or protect consumer data. Preference for one privacy default over another, for example, could restrict innovation because it might deter providers from developing alternative or improved protections for consumer data.

- **Flexibility.** Privacy regulation frameworks should be flexible enough to allow businesses to develop innovative privacy technologies and tools. Flexibility means that businesses can adapt their policies and practices to the contexts in which customer data is used and disclosed and to fit the relationship that a business has with its customers.

- **Certainty.** In addition to having flexible privacy regulation frameworks, businesses must ensure that their implementation of privacy settings meets international standards. Multiple default requirements that are contradictory or are not properly harmonized internationally will slow development and create uncertainty in the release of new products and services. Regulators should encourage innovators to assess the full spectrum of potential privacy risks and make appropriate decisions about privacy designs and settings.

Helpful Resources

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

Privacy by Default: Microsoft's perspective and approach
aka.ms/PrivacyDefault

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

Privacy in Action
www.microsoft.com/yourprivacy

February 2013

Privacy Impact Assessments

Key Points

- A Privacy Impact Assessment (PIA) is defined by European regulators as a "systematic process for evaluating the potential effects on privacy of a project, initiative, or proposed system or scheme and finding ways to mitigate or avoid any adverse effects."
- Microsoft uses a privacy review process for new services and products that is generally equivalent to what many organizations refer to as a PIA.
- PIA frameworks should be required only where appropriate, and should be flexible enough to enable businesses to develop innovative technologies and tools.

BACKGROUND

Privacy Impact Assessments (PIAs) have emerged in recent years as an important mechanism for assessing and minimizing privacy risk to individuals. The EU PIA Framework Project defines a PIA as a "systematic process for evaluating the potential effects on privacy of a project, initiative, or proposed system or scheme and finding ways to mitigate or avoid any adverse effects."

Government agencies developed PIAs in the early 1990s in countries such as the United States, Australia, and Canada. In recent years, the use of PIAs has spread to private companies as well as many countries in Europe and Asia.

There are a number of reasons for conducting a PIA, such as those outlined by the U.K. Information Commissioner's Office: identifying privacy risks to individuals; identifying privacy and compliance liabilities for organizations; protecting an organization's reputation; instilling public trust and confidence in a product or service; and avoiding expensive resolutions to privacy problems discovered later.

Though PIAs vary widely, a 2007 study by Loughborough University in the United Kingdom found four common elements. Conducting a PIA elicits a prospective identification of privacy issues or risks before systems and programs are put in place or modified, and assesses the impacts in terms broader than those of legal compliance. In addition, PIAs are process- rather than output-oriented, and are systematic.

MICROSOFT APPROACH

Microsoft uses a privacy review process that is generally equivalent to what many organizations refer to as a PIA. The Microsoft privacy review process analyzes and determines the privacy requirements and risks of its products and services early on. This process also provides a series of checks and balances to help ensure that the end products comply with Microsoft's privacy principles and policies.

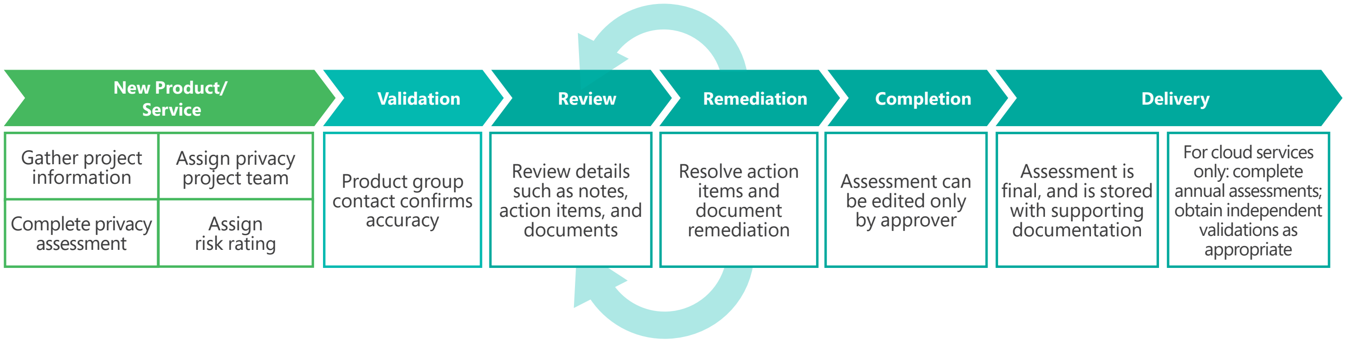
The Microsoft privacy review process follows these phases (illustrated below):

- **Risk assessment.** The first step in Microsoft's typical privacy review process is an assessment that produces a rating of the privacy risk of the product or service.
- **Validation.** The privacy and development teams work together to validate this rating. As the development team designs and builds the product, it may undergo additional privacy assessments.
- **Review and remediation.** During the review and remediation phases, the development team may identify further steps necessary to minimize privacy risks and then implement them. These steps may be repeated many times during product development, until the identified privacy risks have been addressed.
- **Completion and delivery.** Once the product or service is completed, Microsoft conducts a final assessment to determine if all the privacy requirements have been met. If they have, approval is granted. Independent validations and audits may also take place depending on the service.

The privacy review at Microsoft is facilitated through the development and deployment of internal tools that help determine what information is required to complete each review. These internal tools also track the evolution of the product's privacy requirements as it moves from concept to release. They also help the company manage reviews of a wide range of products, including packaged software, Internet services, and web-based marketing campaigns.

POLICY CONSIDERATIONS

- **Selective use.** In some circumstances, it may make sense for regulatory authorities to require the use of PIAs. However, the mandatory use of PIAs for a widespread set of circumstances will likely add unnecessary cost and complexity to the development of products.
- **Flexibility.** PIA frameworks should be flexible and avoid being overly prescriptive to allow businesses to develop innovative privacy technologies and tools. Flexibility means that businesses can adapt their policies and practices to match the contexts in which consumer data is used or shared and the type of relationship they have with the consumer. PIA frameworks should also avoid relying on third parties to conduct PIAs, because the use of third parties works against an environment of transparency and openness between regulators and organizations.
- **Incentives.** One way of encouraging PIAs and robust privacy protection without being overly prescriptive is by offering clear incentives for companies to act responsibly. Accountable controllers could, for example, benefit from less prescriptive requirements or simplified mechanisms to transfer data.
- **Share best practices.** Industry and government should share best practices regarding PIAs and other kinds of privacy review processes. Microsoft makes *Privacy Guidelines for Developing Software Products and Services* publicly available, and has also published *Privacy from the Ground Up*, a white paper that details Microsoft's approach to the many privacy reviews the company conducts annually.



New Product/ Service

Gather project information

Assign privacy project team

Complete privacy assessment

Assign risk rating

Validation

Product group contact confirms accuracy

Review

Review details such as notes, action items, and documents

Remediation

Resolve action items and document remediation

Completion

Assessment can be edited only by approver

Delivery

Assessment is final, and is stored with supporting documentation

For cloud services only: complete annual assessments; obtain independent validations as appropriate

Helpful Resources

An overview of Microsoft privacy policies and initiatives, and a collection of current white papers
www.microsoft.com/privacy

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

The European Union Privacy Impact Assessment Framework Project
www.piafproject.eu

February 2013

Privacy in the Cloud: Office 365

Key Points

- The advances and increased adoption of cloud computing raise important policy considerations, including shared data storage, geographic location, transparency, access, and security.

- Microsoft understands that strong privacy protections are essential for building trust in the cloud and helping cloud computing reach its full potential. So Microsoft built its Office 365 online collaboration service from the beginning with strong data protection in mind, including the dedication of a team of privacy professionals.

- Conflicting legal obligations and competing claims of governmental jurisdiction over data usage continue to limit cloud computing services and their adoption. Divergent rules on privacy, data retention, and other issues cause ambiguity and create significant legal challenges.

BACKGROUND

Cloud computing—Internet-based data storage, processing, and services—is now both a viable alternative and a complement to the traditional model of running software and storing data on premises or on personal devices. Although cloud computing provides convenient, shared access to apps and online services, servers, networks, and storage, this data model raises important privacy and security policy considerations:

- **Shared data storage.** When the data from many customers is stored at a shared physical location, cloud providers must take appropriate steps to segregate that data to protect it from inappropriate use or loss. Additional safeguards include providing strong levels of encryption and proper controls for administrative access.

- **Transparency and access.** Customers want to know where their data is stored, who has access to it, how it is used and shared, and what safeguards are protecting it. Cloud providers can address these concerns—and build trust, too—by implementing transparent policies and communicating them clearly to customers and regulators.

- **Geographic location of data.** As cloud computing evolves, traditional geographical limits on data storage and movement also shift. For instance, data created in France using software hosted in Ireland could be stored in the Netherlands and accessed from the United States. Consequently, regulators and cloud computing customers want clearly defined policies and disclosures regarding the physical location of their data.

- **Security.** Customers rely upon their cloud service providers not only to store their data securely but also to keep it safe from loss, theft, or misuse.

MICROSOFT APPROACH

Microsoft offers a number of cloud-based products, including Microsoft Office 365, a service that provides access to cloud-based email, web conferencing, file sharing, and Office Web Apps.

Microsoft understands that strong privacy protections are essential for building trust in cloud computing, and implements them in Office 365 as follows:

Data use. Microsoft explains clearly how it manages and uses customer data, including explicit statements that Microsoft uses it only for maintaining and securing Office 365 services. Office 365 does not use customer data—for example, by scanning email or documents stored in the cloud—to create advertisements.

Shared data storage. To enable cost savings and efficiencies for data storage, Microsoft stores customer data from multiple customers on the same equipment (known as a *multi-tenant format*). However, the company goes to great lengths to help ensure that multi-tenant deployments of Office 365 logically separate the data (and processing) of different accounts and support the privacy and security of the data stored.

Data portability. Microsoft enables Office 365 customers to export any or all of their data at any time and for any reason, without any assistance from Microsoft. Even after an Office 365 account expires or is closed, customers by default have limited access for an additional 90 days to export data.

Transparency. The Office 365 Trust Center details the policies and practices that the Office 365 service uses to protect customer data.

Security. Microsoft helps protect Office 365 with a security regimen that includes daily monitoring.

Access. Microsoft identifies any of its subcontractors who can access customer data and the circumstances under which they can access it. The company also logs and reports any access to critical data. Additionally, Microsoft and its third-party auditors conduct sample audits to help ensure that the customer's data is accessed only for appropriate business purposes.

Geographic location of data. For customers interested in knowing where their data is stored, including the assignment of private storage locations, Microsoft tells customers where the major data centers are located, and how it determines where data is stored. Office 365 administrators can also choose to receive updates to changes in data center locations.

POLICY CONSIDERATIONS

- Conflicting legal obligations and competing claims of governmental jurisdiction over the use of data continue to limit cloud computing services and their adoption. Divergent rules on privacy, data retention, and other issues cause ambiguity and create significant legal challenges.

- Microsoft supports privacy legislation that facilitates the free flow of information, builds trust, and encourages innovation. Because data flows are global, the company strives to harmonize privacy regulations, policies, and standards worldwide.

- As governments develop policies that address the privacy and security concerns associated with such emerging technologies as cloud computing, they should continue to support technological innovation and its adoption. Working together, government and industry can establish appropriate privacy principles that protect data in the cloud.

Helpful Resources

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

Microsoft Office 365
office365.microsoft.com

Privacy and cloud computing at Microsoft
www.microsoft.com/privacy/cloudcomputing.aspx

The Office 365 Trust Center
www.trust.office365.com

February 2013

Online Safety

Key Points

- The Internet enriches lives in many ways, but it also presents risks to privacy, safety, personal and professional reputations, and commerce—due, in part, to the online presence of cyber criminals, online bullies, and malicious software.
- Microsoft's approach to online safety includes technology tools; education and guidance; and partnerships with government, industry, law enforcement, and other key organizations to help create safer, more trusted computing experiences.
- Online safety is a shared responsibility, and government and industry should work together to support this objective. Technology companies, governments, businesses, and consumers can partner to innovate, develop, and deploy effective solutions.

BACKGROUND

The Internet has revolutionized the ways that consumers work, learn, communicate, and play. At the same time, the Internet has also created new risks and new potentials for harm. These include infection by malicious software, such as viruses, worms, and spyware; victimization by online scammers selling counterfeit goods or pushing fraudulent investment schemes; loss of privacy and damage to online reputation; identity theft by criminals; and unwanted contact from spammers and other individuals with malicious intentions.

Consumers are concerned about these risks and are taking steps to protect themselves. A Microsoft research report[1] released in 2011 found that 90 percent of adults and youth in the United States and four European countries have taken some steps to manage their online profiles. However, only 44 percent of adults and youth reported actively thinking about the long-term consequences that their online activities may have on their reputations and identities.

While consumers are actively working to protect themselves, they also have high expectations that industry and government will work to make the online world more secure. If companies fail to meet these expectations, consumers will be less inclined to use online technologies, and both industry and individuals will suffer from a lack of trust.

The unique challenges of online safety require a coordinated response. Technology companies, governments, businesses, and consumers must work together to innovate, develop, and deploy effective solutions. Technology companies must be committed to creating a safer and more trusted Internet. Sensitive data and personal information must be protected, and technology should facilitate business practices that promote trust. Microsoft believes that addressing these present and future challenges requires the collaborative efforts of technology companies, governments, consumers, and businesses.

[1] *Teen Online Reputation: 13-17 Years Old*
www.microsoft.com/security/resources/research.aspx#teen

MICROSOFT APPROACH

Microsoft takes a three-pronged approach to helping create safer, more trusted computing experiences.

- **Technology tools.** Microsoft offers a number of online safety tools, including Microsoft Security Essentials, a free antimalware program. Microsoft enables all Microsoft account holders to specify who can view their profiles, who can contact them, and who can post or view the content they share. Microsoft Family Safety provides tools that help parents monitor and protect children online, and Xbox 360 comes equipped with Console Safety Settings.

- **Education and guidance.** The Microsoft Safety & Security Center provides guidance for safer Internet use. It offers tips and advice on how people can better secure their computers, protect their online reputations, avoid online scams, help secure their mobile devices, and avoid, block, and report inappropriate behavior.

- **Partnerships.** Creating a safer and more trusted online environment requires a holistic approach in which consumers, government leaders, technology providers, and non-governmental organizations (NGOs) all play a vital role. Central to Microsoft's focus is engaging, through public policy, with governments around the world and with NGOs such as the National Cyber Security Alliance.

POLICY CONSIDERATIONS

- **Support public and private partnerships.** Microsoft believes public and private partnerships are essential to address the increasing complexities of cyber crime. The company works with law enforcement agencies by providing them with technical training and by developing new technology tools to combat cyber crime. Microsoft also helps protect consumers through legal action to stop cyber criminals, including actions to shut down botnets, and by bringing legal action against the purveyors of fake security software. Other efforts involve developing and sharing PhotoDNA, a technology that helps industry and government find and remove some of the worst images of child sexual exploitation from the Internet.

- **Support industry self-regulation and legislative frameworks.** As governments address the risks associated with emerging technologies and online services, it is important that they foster an environment of technological innovation in the process. Government and industry can work together to establish safety principles and allow service providers to help fulfill those promises. Examples include the Safer Social Networking Principles for the European Union and an ISP code of practice in Australia.

- **Commission studies and fund research to advance Internet safety.** Research plays a critical role in identifying factors that increase online risks and in dispelling myths that can lead to misplaced efforts. Government funding is essential for both academic and industry research in these areas.

- **Online safety education in schools.** Microsoft believes that online safety curricula should become an integral part of schools' efforts to achieve technological literacy for their students, and should include modules focusing on online safety, online security, and online ethics.

Helpful Resources

Microsoft Security & Safety Center with online safety guidance
www.microsoft.com/security

Online Fraud: Your Guide to Prevention, Detection, and Recovery
aka.ms/OnlineFraudBooklet

Security tips and advice from the National Cyber Security Alliance
www.staysafeonline.org/

February 2013

Child Online Safety

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 technology tools; education and guidance; robust internal policies and practices for moderating content and addressing online abuses; and partnerships with government, industry, law enforcement, and others to help create safer, more trusted computing experiences for everyone.

- Online safety is a community challenge, and government, industry, and others should work together to establish and implement safety principles. As governments address risks associated with emerging technologies and online services, it is important that they continue to encourage innovation and technology adoption in the process.

BACKGROUND

While the Internet provides access to a wealth of positive experiences for children, parents face challenges in monitoring the content their children encounter online, the people they meet there, and what they share. 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 or embarrassing images.

- **Inappropriate contact.** Adults can use the Internet to find and approach vulnerable youth. Frequently, their goal is to develop what youth believe to be meaningful online relationships, a process referred to as grooming.

MICROSOFT APPROACH

Microsoft takes a four-part approach to children's online safety:

- **Technology tools.** Parents can work to minimize online risks by using safety features built into a wide range of Microsoft products and services. For example, Microsoft Family Safety provides tools that help parents monitor and protect children online. Microsoft enables Microsoft account holders to specify who can view their profiles or contact them. In addition, Xbox 360 comes equipped with Console Safety Settings.

- **Internal policies and practices.** Company-wide policies, standards, and procedures in the development of Microsoft products and services that connect with the web 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.

- **Partnerships.** In Microsoft's 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.

- **Education and guidance.** The Microsoft Safety & Security Center provides age-based guidance for Internet use, including tips on how to teach children what's appropriate to view and share online. The site offers guidance on such issues as online bullying, safer social networking, mobile device safety, 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 & 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 and legislative frameworks.** 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. In addition, government and industry must collaborate to establish safety principles and help offer a more secure online environment for youth. Examples of this collaboration include the Safer Social Networking Principles for the European Union, an ISP code of practice in Australia, and the European Union's CEO Coalition on Child Online Safety.

- **Promote integration of Internet safety education into school curricula and teacher training.** Microsoft believes that students and teachers can benefit from Internet safety education that teaches them how to avoid online dangers, protect their devices, and conduct themselves ethically on the web. The company encourages governments to work 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 to advance Internet safety. Government funding for both academic and industry research in these areas is essential.

Helpful Resources

Microsoft Security & Safety Center with age-based guidelines for Internet use
www.microsoft.com/security

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

The Family Online Safety Institute
www.fosi.org

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

February 2013

Combating Human Trafficking

Key Points

- While technology can be used to facilitate the insidious practice of human trafficking, technology can also help combat it.
- Microsoft applies its experience in addressing technology-facilitated crime and investing in research, programs, and partnerships to support human rights and advance the fight against human trafficking.
- Issues related to human trafficking are complex and require a multi-part solution, including strong public-private partnerships and intervention efforts founded in solid research.

BACKGROUND

Human trafficking includes commercial sexual exploitation, forced labor, and other forms of modern-day slavery, and technology can play a role both in facilitating and combating these horrific human rights abuses. Currently, there is insufficient research data to determine the extent to which technology is increasing human trafficking, or to what degree law enforcement and non-governmental organizations (NGOs) can use technology to better identify perpetrators and victims. However, advances in research and data sharing suggest that there is great potential in using technology to help address trafficking.

Anti-trafficking advocates, law enforcement agencies, and governments around the world have long been working to combat human trafficking. As with the fight against other forms of technology-facilitated crime, Microsoft believes technology companies also have an important role to play in driving deeper research and innovation to use technology to more effectively disrupt the trafficking of people.

MICROSOFT APPROACH

Microsoft recognizes its responsibility as a global corporate citizen to respect human rights and aid in the fight against human trafficking. Microsoft expresses its commitment in the Human Rights statement it released in July 2012 in accordance with the United Nations Guiding Principles on Business and Human Rights.

The company puts its commitment into action through the collaborative efforts of Microsoft Research, the Microsoft Digital Crimes Unit, and the newly established Microsoft Technology and Human Rights Center. Efforts include:

Research and innovation. Microsoft invests in research to develop a more accurate understanding of the role that technology plays in child sex trafficking in particular.

- In December 2011, Microsoft Research and the Digital Crimes Unit issued a request for proposals for academic research into the role of technology in the sex trafficking of children. Microsoft distributed $185,000 to six winning teams whose research results are anticipated later in 2013.

- Microsoft is collaborating with the Harvard Kennedy School of Government and the University of Southern California Annenberg School on additional research.

- Microsoft works with leading technology institutions and NGOs on efforts such as the International Girls Only Hackathon, which helps foster technology innovation directed at addressing trafficking.

Partnerships. Microsoft works with anti-trafficking advocates, such as the International Centre for Missing and Exploited Children, and law enforcement agencies around the world to help protect children against technology-facilitated sexual exploitation. PhotoDNA, an image-matching technology partially developed by Microsoft is used by NGOs, law enforcement, and other technology companies like Facebook and NetClean to help identify images of child abuse.

Microsoft collaborates on public-private initiatives to address human trafficking with the Global Business Coalition Against Trafficking, the White House Office of Science and Technology Policy, the Council on Women and Girls, UN.GIFT, U.S. state attorneys general, and local police agencies.

In September 2010, Microsoft joined the Thorn Foundation as a founding member of a technology task force with Facebook, Twitter, Google, and others to explore new ways technology can address the child sex trafficking problem. In addition, Microsoft supports NGOs that combat trafficking and support its victims, such as the Polaris Project and the International Justice Mission.

Disruption. Microsoft believes that disruptive action plays an important role in shifting the dynamics that fuel the trade of human trafficking. Through cooperative efforts that raise the cost, risk, and difficulty of doing business for traffickers, Microsoft can help make it a less lucrative, and therefore less appealing, trade.

Policies and best practices. Microsoft works to help prevent its technologies and processes from contributing to exploitation in its operations and those of its suppliers.

All companies doing business with Microsoft must agree to abide by the company's Vendor Code of Conduct, which outlines required ethical business practices, including an explicit prohibition of the use of forced labor. For its hardware manufacturers and packaging suppliers, Microsoft has invested in a social and environmental accountability program, which includes independent third-party auditing to help ensure compliance with its Code of Conduct and local and national regulations. If these standards are not met, suppliers risk remedial action including termination of their contracts.

Microsoft also uses such technologies as PhotoDNA on Bing and SkyDrive to help mitigate the use of its online services for the exploitation of children and distribution of child pornography.

POLICY CONSIDERATIONS

- Microsoft supports enacting and enforcing human trafficking laws that recognize and protect victims while holding traffickers accountable.

- Researchers and technology companies should continue to work with governments, law enforcement, and those in the anti-trafficking community to help understand and address the abuses of technology that facilitate trafficking, look for effective intervention techniques based on research, and develop anti-trafficking initiatives.

- The technology industry can establish best practices that include investment in scientific research, enforcement of codes of conduct, the provision of mechanisms for customers to report potential problems, and promotion of trafficking hotlines and information for victims.

Helpful Resources

Microsoft's human rights statement
aka.ms/Human-Rights-Statement

Microsoft's research initiative on the role of technology in child sex trafficking
aka.ms/human-trafficking-rfp

Microsoft Digital Crimes Unit
www.microsoft.com/dcu

Microsoft Research
research.microsoft.com

Microsoft PhotoDNA
www.microsoftphotodna.com

Global Business Coalition Against Trafficking
gbcat.org

February 2013

Combating Child Exploitation Online

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 through child pornography.
- Microsoft devotes extensive resources in advancing technology, techniques, and processes to combat the use of the Internet to exploit children. These include filtering tools and an advanced technology, PhotoDNA, that helps refine and automate the search for child pornography among the billions of photos on the Internet.
- Microsoft is working with experts around the world to advance innovations that will combat the sexual exploitation of children, including child pornography and sex trafficking.

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, such as through the distribution of child pornography (also known as child abuse images), the trafficking of children for sex, and the grooming of children for sexual exploitation.

The production and distribution of child pornography represents a significant law enforcement problem. Since 2002, the National Center for Missing & Exploited Children (NCMEC) has reviewed and analyzed more than 65 million photos and videos of child pornography. These images are often found after pedophiles share and trade them among themselves and with others who reinforce their shared sexual interest in children.

As of 2011, most of the victims of child pornography that NCMEC identified were prepubescent, with infants and toddlers the fastest-growing age category. Internet companies have an important role to play in helping fight this horrific trade by acting quickly to find, report, and eliminate these illegal images.

Another form of child exploitation is the use of the Internet by child predators to find 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. As in the fight against child pornography, Internet companies have an important function in stopping predators and child sex traffickers. They can enforce codes of conduct, provide mechanisms for customers to report predators, and invest in innovation for improved detection.

Globally, law enforcement is doing admirable work to combat the online exploitation of children, but the scale of this problem requires broader cooperation across law enforcement, government, industry, non-governmental organizations (NGOs), and academia.

MICROSOFT APPROACH

- The Microsoft Digital Crimes Unit (DCU) is a worldwide team of attorneys, investigators, technical analysts, and other specialists. The team works to transform the fight against digital crime through partnerships and legal and technical breakthroughs that destroy the way cyber criminals operate. DCU is a unique team in the tech industry, focused on disrupting some of the most difficult cyber crime threats facing society today—including the sexual exploitation of children facilitated by technology.

- Microsoft devotes extensive resources to developing technology that battles online child exploitation and that supports the efforts of governments and NGOs devoted to the cause. Microsoft applies filtering tools and employs more than 100 trained experts to help detect and classify images of child abuse using Bing, SkyDrive, and other services. The company reports these images of apparent child pornography to NCMEC, removes them, and bans from the services the individuals or entities responsible for publishing them.

- Among the latest tools Microsoft uses in the fight against these illegal images is an advanced technology called PhotoDNA, developed by Microsoft Research in collaboration with Dartmouth College. It helps to refine and automate the search for child pornography among the billions of photos on the Internet. In 2009, DCU donated the license for PhotoDNA to NCMEC to help it work with online services such as Facebook to uncover images of child abuse.

- Microsoft works with law enforcement agencies around the world to develop tools to support their important work in fighting the exploitation of children. In 2012, Microsoft worked with NetClean to make PhotoDNA image-matching technology available to law enforcement at no cost to aid in investigations of the sexual exploitation of children.

- Microsoft is also working with others to advance innovation in fighting child sex trafficking. The company collaborates with the Thorn Foundation's technology task force (whose members also include Facebook, Twitter, Google, and others), to explore new ways technology can address the problem. In 2012, DCU and Microsoft Research provided grants to six research teams to advance a deeper understanding of the advertising and selling of children and the use of technology in the child sex trade. The release of research results is expected later in 2013.

POLICY CONSIDERATIONS

- Microsoft strongly supports enacting and enforcing laws against the possession, production, and distribution of child pornography worldwide. In 2010, the International Centre for Missing & Exploited Children (ICMEC) reported that only 45 countries have legislation sufficient to fight child pornography—and 89 countries have no laws at all that specifically address it.

- Internet companies should continue to work with governments and law enforcement to help address the problem of online predators by establishing industry best practices and guidance. More emphasis should be placed on how to enable companies to voluntarily find and report child pornography in order to eliminate it from the Internet. Policymakers can help change the focus of law enforcement to a victim-centric model that measures law enforcement on activities that stop crime and prevents victimization.

Helpful Resources

Microsoft Security & Safety Center with age-based guidelines for Internet use
www.microsoft.com/security

Microsoft's PhotoDNA
www.microsoftphotodna.com

The Microsoft Digital Crimes Unit
www.microsoft.com/DCU

Microsoft's human rights statement
aka.ms/Human-Rights-Statement

The National Center for Missing & Exploited Children (NCMEC)
www.ncmec.org

Microsoft's research initiative on the role of technology in the sexual exploitation of children
aka.ms/human-trafficking-rfp

February 2013

Combating Child Grooming on the Internet

Key Points

- Grooming, the process by which predators manipulate children for sexual exploitation, is facilitated online when sexual predators use the Internet to make contact and develop relationships with children.

- Microsoft's approach to combating child predation includes innovative technology tools, education and guidance, internal policies and practices for moderating content and addressing online abuses, and relationships with government, industry, and law enforcement.

- Microsoft strongly supports enacting and enforcing laws against the sexual exploitation of children, and cooperates with law enforcement to bring Internet pedophiles to justice.

BACKGROUND

Child grooming is a process of emotional manipulation by which pedophiles prepare children and youth for sexual exploitation. The grooming process typically involves an adult befriending a young person and then winning his or her trust by showering the youth with flattery, sympathy, gifts of money or modeling jobs, and other personal attention. Finally, the groomer attempts to sexualize the relationship, seeking to control the child and continue the abuse, which may include child pornography or even sex trafficking.

Pedophiles go where children go—and today that includes the Internet. Child grooming goes online when pedophiles use the Internet for the grooming process. Adults may begin the grooming process by visiting forums where youth interact, such as online games (which may use two-way voice and video technology) or chat rooms, or contact children through text messages. Pedophiles may use the information that children reveal about themselves online and target vulnerable youngsters with low self-esteem, family problems, or lack of money.

Sexual exploitation of children is a global problem. However, it is important to keep the online portion of the problem in perspective. According to the Crimes Against Children Research Center in the United States, the arrest of more than 600 online predators in 2006 constituted about 1 percent of all arrests for sex crimes committed against children and youth.

Internet companies have an important role to play in helping to stop predators. They can enforce codes of conduct, deploy monitors in forums used by children, and provide mechanisms for customers to report potential predators.

MICROSOFT APPROACH

Technology tools. Parents can watch over their children online by using safety features built into a wide range of Microsoft products and services.

For example, Windows 8 Family Safety provides tools to help parents monitor their children's online activities. Anyone—adult or young person—with a Microsoft account can specify who can view their profiles or contact them. In addition, Xbox LIVE has Online Safety Settings that enable parents to restrict who children can communicate with and who can see their profiles or friends lists.

Internal policies and practices. To protect users of its online services, Microsoft enforces policies such as a code of conduct, and moderates content and interactions to address illegal activity, inappropriate material, and other abuse.

Partnerships. Combating child predation requires a holistic approach in which technology providers, government leaders, law enforcement, and non-governmental organizations all play vital roles.

- Central to Microsoft's efforts is the Microsoft Digital Crimes Unit (DCU), a worldwide team of lawyers, investigators, technical analysts, and other specialists whose focus includes advancing the fight against the sexual exploitation of children online. To fight cyber criminals, the DCU team forges relationships with leaders in a variety of fields and uses new legal and technical tools.
- Microsoft works with the International Center for Missing & Exploited Children, INTERPOL, and other organizations to encourage governments to combat child predators.

Education and guidance. The Microsoft Safety & Security Center provides age-based guidance for Internet use, including tips on teaching children what's appropriate to view and share online, how to stay safer on mobile devices and in online games, and how to avoid, block, and report inappropriate behavior.

POLICY CONSIDERATIONS

- Microsoft strongly supports enacting and enforcing laws against the sexual exploitation of children, including the possession, production, and distribution of child pornography.
- Internet companies should continue to work with governments and law enforcement to help address the problem of child predators online by giving their customers mechanisms for reporting potential predators, enforcing codes of conduct, supporting law enforcement, and spurring further innovation.
- It is essential that governments commission studies and fund academic and industry 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 to advance Internet safety.

Helpful Resources

Microsoft Security & Safety Center resources for youth safety online
aka.ms/young-safety

Comparison of Microsoft family safety tools
aka.ms/compare-tools

Microsoft's research initiative on the role of technology in human trafficking
aka.ms/human-trafficking-rfp

Crimes Against Children Research Center
www.unh.edu/ccrc

International Centre for Missing and Exploited Children
www.icmec.org

February 2013

Combating Online Fraud

Key Points

- Online fraud is a significant global problem, victimizing millions of unsuspecting consumers each year. In the United States alone, the FBI's Internet Crime Complaint Center recorded 300,000 fraud complaints in 2011 with an adjusted dollar loss of nearly half a billion dollars.

- Microsoft's four-part approach to combating online fraud includes dedicated internal teams, technology tools, education and guidance, and relationships with government, industry, law enforcement, and others.

- Microsoft supports government efforts to fight online fraud through international cooperation, public and private relationships, and strong enforcement of anti-fraud laws.

BACKGROUND

The Internet has transformed commerce around the world, allowing people to enrich their lives, build new companies and services, and engage in a wide variety of economic activities. Total global e-commerce sales are projected to exceed $1.2 trillion in 2013.

However, as economic activity moves increasingly online, so has the problem of fraud, which threatens to undermine the public trust in the benefits of e-commerce.

Online fraud is a significant global problem, victimizing millions of unsuspecting consumers each year. In the United States alone, the FBI's Internet Crime Complaint Center recorded 300,000 fraud complaints in 2011 with an adjusted loss of nearly half a billion dollars. Organized groups of cyber criminals go to great lengths to perpetrate their schemes to steal identities or commit financial fraud.

Online fraud schemes lure their victims using such devious tactics as social engineering, malicious software, and other attacks that victimize millions of individuals every year.

Social engineering takes advantage of people's trust by tricking them into such actions as installing malicious software disguised as a legitimate app or entering sensitive personal information on a convincing but fake website—actions that can compromise their computer or data.

Scams that use email, text, or social network messages that appear to come from a reputable organization and entice victims to disclose information such as account numbers or passwords are known as *phishing*. Research shows that they pose a threat to consumers. In 2011, the Anti-Phishing Working Group reported nearly 200,000 unique phishing attacks worldwide, and its recent data shows that the number of brands being exploited by phishers is at an all-time high.

To combat online fraud successfully, businesses, government, non-governmental organizations, and consumers worldwide can work together to fight it.

MICROSOFT APPROACH

Microsoft's four-part approach to combating online fraud includes dedicated internal teams, technology tools, education and guidance, and relationships with government, industry, law enforcement, and others.

- **Dedicated internal teams.** The Microsoft Digital Crimes Unit (DCU) is a worldwide team of attorneys, investigators, technical analysts, and other specialists. The team fights digital crime through relationships and legal and technical breakthroughs that destroy the way cyber criminals operate. DCU is a unique team in the tech industry, focused on disrupting some of the most difficult cyber crime threats facing society today—including the sexual exploitation of children facilitated by technology.

- **Technology tools.** Microsoft offers many online safety tools to help consumers fight online fraud, including Microsoft Security Essentials, a free antimalware program, as well as SmartScreen technologies and services.
  - » The SmartScreen service helps protect consumers against downloading malware from social engineering tactics such as phishing in Windows Internet Explorer 9 and 10.
  - » The SmartScreen Application Reputation service helps Internet Explorer 9 and 10 customers make better decisions about the trustworthiness of programs they download. When a user downloads an app from the Internet, SmartScreen uses reputation data to remove unnecessary warnings for well-known files and to show warnings when the download is at a higher risk of being malicious.
  - » SmartScreen antispam technologies and services help to protect Microsoft customers from email that may contain fraudulent solicitations.

- **Education and guidance.** The Microsoft Safety & Security Center provides guidance for safer Internet use, including tips on how consumers can secure their computers and avoid online scams.

- **Partnerships.** Microsoft works with many organizations dedicated to fighting online fraud, including the Anti-Phishing Working Group and the National Cyber Security Alliance.

POLICY CONSIDERATIONS

- **International cooperation.** Microsoft has joined with industry 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 online crime.

- **Public and private relationships.** Microsoft believes public and private relationships are essential to addressing the increasing complexities of cyber crime. Microsoft gives technical training to law enforcement agencies worldwide and develops new technologies to combat cyber crime. Microsoft has also helped protect consumers through legal action.

- **Strong enforcement and balanced regulation.** Microsoft strongly supports the enactment and enforcement of laws against online fraud, and the prosecution of cyber criminals. At the same time, it is important that legislation be carefully crafted so as not to discourage innovation and technology adoption in the process.

Helpful Resources

The Microsoft Safety & Security Center with guidance for consumers
www.microsoft.com/security

Online Fraud: Your Guide to Prevention, Detection, and Recovery
aka.ms/OnlineFraudBooklet

The Microsoft Digital Crimes Unit
www.microsoft.com/dcu

February 2013

Digital Citizenship

Key Points

- Today's young people are navigating a new digital culture in which rules and social norms are sometimes unclear. They must learn about digital citizenship—and develop a sense of ownership and personal responsibility—in order to make responsible, ethical decisions in the online world.

- The Internet presents great opportunities for young people, but not without real risks. Some of the risks can be mitigated by helping young people develop a strong sense of digital citizenship.

- Rather than relying solely on protective measures that are primarily reactive responses to existing problems, an approach to online safety that includes proactively teaching digital citizenship will help young people safely interact in the online world. Teaching young people about digital literacy, ethics, and etiquette is no longer merely an option—it is an imperative.

BACKGROUND

New information technologies have profoundly changed the world in which today's young people learn and grow. The immense resources of the Internet and the accompanying array of Internet-enabled devices give young people tremendous opportunities to learn, share, and communicate. Yet adults have concerns about online safety for young people, who might encounter inappropriate content or sexual predators, suffer damage to their online reputations, or have other harmful experiences online.

Many countries have implemented a three-part approach to protecting young people with technology tools, safety education, and law enforcement activities. All three play vital roles, but these strategies are often reactive responses to emerging safety issues. A more proactive and comprehensive approach to online safety would include measures that take into account the rules and behaviors that young people must understand before they can become responsible digital citizens. Digital citizenship takes just such an approach.

Digital citizenship is often defined as "the norms of behavior with regard to technology use." But digital citizenship is about more than social norms—it is about preparing young people for living and learning in a technology-rich society. Digital citizenship helps young people develop a sense of ownership and personal responsibility that, in turn, will help them make appropriate, ethical decisions in the online world. It has two primary elements:

- **Digital literacy.** Young people who are literate in the online world will have a better chance of avoiding risky situations, will make better-informed decisions, and will better understand how to protect their privacy. But digital literacy involves more than mere technical competence—it requires critical thinking skills to evaluate many different sources of digital information.

- **Digital ethics and etiquette.** While technical knowledge provides a solid foundation for digital citizenship, young people must also learn digital ethics and etiquette before they can make sound decisions in the online world. Instruction in digital ethics will help young people make good ethical decisions, and instruction in digital etiquette will help them operate within online social norms.

MICROSOFT APPROACH

- Microsoft's approach to children's online safety includes technology tools, education and guidance, and partnering with government, industry, law enforcement, and others to help create safer, more trusted computing experiences for everyone.

- Microsoft supports the integration of digital citizenship in technology instruction for students. Given the pervasiveness of technology in classrooms today, Microsoft believes that digital citizenship is an important component of any school curriculum.

- The Microsoft Safety & Security Center provides age-appropriate guidance for Internet use, including tips for teaching children what's appropriate to view and share online. The site provides information about topics including the prevention of online bullying, safer social networking, safe use of mobile devices, responsible online gaming, and addressing inappropriate online behavior.

POLICY CONSIDERATIONS

- Microsoft supports broadening online safety efforts to include an emphasis on digital citizenship through digital media literacy and education programs that help parents and teachers prepare kids for navigating online and managing digital media.

- Microsoft suggests that education policymakers adopt a set of national goals for online safety, including minimum standards for digital literacy curricula, to better educate children and families about managing multimedia-infused lives.

- Although there are many things that governments should do, it is important to note what they should not do. It is tempting to try to protect young people with legislation that imposes technology mandates. These, however, have generally proven ineffective, especially given the global reach and scale of the Internet. Further, mandated technology may quickly become obsolete due to the fast-paced and ever-changing nature of the digital world.

Helpful Resources

The Microsoft Safety & Security Center, with age-based guidelines for Internet use
www.microsoft.com/security

Online Safety 3.0: Empowering and Protecting Youth
aka.ms/Online-Safety30

The Family Online Safety Institute
www.fosi.org

Research and curriculum materials promoting digital citizenship
www.digitalcitizenship.net

February 2013

Parental Controls

Key Points

- Parental controls play an important role in online safety for many families. While not a substitute for parental involvement, monitoring, filtering, and other such technologies can help reduce the risk of exposure to inappropriate content, contact, and conduct.

- Microsoft helps meet the needs of parents and caregivers by providing online safety and privacy features in a number of its products, including Windows 8, Xbox 360, and Windows Phone 8.

- Microsoft believes that decisions about what children view and do online are best left to parents and caregivers. Microsoft encourages government to work with industry and non-governmental organizations (NGOs) to help promote and publicize online safety technology.

BACKGROUND

While the Internet offers many enriching opportunities for young people, there are also concerns—inappropriate content, contact, and conduct (such as bullying and harassment). Societies have struggled with how best to protect youth online while respecting the rights of adults to freely access information and preserving an open and prosperous Internet.

One way to help protect youth is through technologies that parents and caregivers can use to monitor and control children's online activities. These technologies—including filtering content, restricting the download and use of music, apps, and other files, and managing contacts—have been used on personal computers since the early 1990s. Now, as mobile phones, media players, e-readers, and gaming consoles have become Internet-enabled, technology companies have added such parental controls to these devices as well.

Parental controls are widely used in many countries. In 2011, a survey by the Family Online Safety Institute[1] found that 54 percent of parents in the United States used them; research[2] by the European Commission indicated adoption by 53 percent of parents in the United Kingdom.

Despite their popularity and obvious utility, however, parental controls have generated controversy. Some have advocated that governments should mandate their use by minors (and even everyone), a position that human rights advocates and others strongly oppose. Others raise concerns about the misuse of such technology for spying by overzealous parents, controlling employers, and possessive spouses, or for censorship by repressive governments.

Companies that create parental control technologies must balance providing robust tools that empower parents and caregivers to best manage Internet access and use in their families, while respecting free expression and protecting privacy.

[1] *Who Needs Parental Controls? A Survey of Awareness, Attitudes, and Use of Online Parental Controls*
www.fosi.org/research/900-who-needs-parental-controls.html

[2] *EU Kids Online*
aka.ms/EUKidsOnlineReport

MICROSOFT APPROACH

For years, Microsoft has worked to protect families by providing safety and privacy features in such products as the Windows operating system, Xbox, Xbox 360, Windows Phone, and Bing. Microsoft believes that the company's role in providing parental controls is not to decide what others may view, but rather to give families the tools to implement their own decisions.

- **Windows 8: Microsoft Family Safety.** Family Safety enhances the standard parental controls in Windows (such as web filtering, blocking inappropriate content, and time and program restrictions) with a central online location, the Family Safety website. There parents can manage settings for the computers of every family member and view reports of their online activity.
- **Windows Phone 8: Kid's Corner.** A new feature in Windows Phone 8, Kid's Corner enables parents and caregivers to create special accounts for children that can limit access to apps, games, videos, and music. The child can enjoy these on Kid's Corner on the parent's phone, but won't be able to access functions that might not be age appropriate, such as web browsing or text messaging, or important apps or files.
- **Xbox 360 and Xbox LIVE.** Microsoft was the first gaming console to introduce ratings-based parental controls, Family Settings, for Xbox 360 (the Microsoft video game and entertainment system) and Xbox LIVE (Microsoft's online entertainment service).
    - Console Safety Settings help parents decide and enforce what their children can play, online and off, based on content ratings for games, movies, and television shows, and set limits on console play time using the Family Timer.
    - Online Safety Settings enable parents to create a profile for each child to help ensure that content is appropriate for his or her age and maturity level. Parents can specify the child's activities, including multiplayer gaming, video chat, and voice or text messaging. They can also restrict who children can communicate with, and who can see their profiles or friends lists.

POLICY CONSIDERATIONS

- Microsoft believes that decisions about what children can view online are best left to parents and caregivers. Microsoft does not support efforts to require the use of parental controls or filtering software. Instead the company encourages government to work with industry and non-governmental organizations (NGOs) to help promote and publicize online safety technology. GetNetWise is one such nonprofit organization, which offers guidance and tools to address the latest safety issues for kids online.
- Microsoft supports industry self-regulation as well as thoughtful legislative frameworks in emerging technology areas. As governments address risks associated with emerging technologies and online services, it is important that they allow for innovation in the process.
- Government and industry can work together to establish safety principles and help create a more secure online environment. Examples of this collaboration include the Safer Social Networking Principles for the European Union and the development of an ISP code of practice in Australia.
- Microsoft supports legislation that provides a safe haven for companies that engage in online moderation of behavior and content by not increasing their liability for engaging in that moderation. Examples include Section 230 of the U.S. Communications Decency Act and the European Union Directive 2000/31/EC.

Helpful Resources

Microsoft Security & Safety Center safety guidelines for the whole family
www.microsoft.com/security/family-safety

Microsoft Family Safety software
aka.ms/Microsoft-family-safety

Safety resources for video games and online media
www.GetGameSmart.com

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

February 2013

Mobile Devices and Youth Safety

Key Points

- Mobile phones are widely used by young people, and they have become an important means of communication for families worldwide. However, mobile phones also pose safety concerns such as inappropriate content, conduct, contact, and commerce.
- Microsoft offers a number of safety and privacy features on Windows Phones, including Kid's Corner, which enables parents or caregivers to create a special account for a child where they can set limits on access to apps, games, videos, and music.
- Microsoft supports efforts by mobile providers to establish voluntary industry guidelines and best practices to address such issues as content classification, location-based services, and mobile commerce, and to help customers make decisions that are best suited for their families.

BACKGROUND

In 2011, MobileYouthReport.com estimated that 1.6 billion people under the age of 30 worldwide own a mobile phone. The benefits are clear: mobile phones help parents stay in touch with their children and enable children to connect with their friends. With smartphones, they can also enjoy the Internet and the world of information available there.

Because many mobile phones provide Internet access, children and young subscribers face many of the same issues with a phone as they would with any other Internet-enabled device:

- **Inappropriate content.** Young people may stumble upon inappropriate material including hateful or sexual content by clicking a link in email, on a social network, or on the web.
- **Inappropriate conduct.** Young people may use mobile phones to harass or exploit others. Children can send hurtful, bullying messages or embarrassing images. A particular concern with mobile devices is sexting—the transmission of sexually explicit photographs and videos taken with a mobile phone camera.
- **Inappropriate contact.** Adults and other youth can use the Internet to find and approach vulnerable kids. Frequently, their goal is to develop what youth believe to be meaningful online relationships, a process referred to as grooming.
- **Inappropriate commerce.** Children can easily fall victim to phishing or other scams, and be enticed to click a flashy ad, open an enticing "free" game, or download a ringtone, which may download a virus, spyware, or other malicious software or surprise parents with expensive charges for those mobile devices.

MICROSOFT APPROACH

- Microsoft's approach to children's online safety includes technology tools; education and guidance; robust internal policies and practices for moderating content and addressing online abuse; and relationships with government, industry, law enforcement, and others to help create safer, more trusted computing experiences.
- To help promote mobile safety for children and young people, Microsoft works with industry and non-governmental organizations that include the GSM Association, CTIA – The Wireless Association, and the Family Online Safety Institute.
- Windows Phone users can control a number of features that impact their privacy by using the **Express Settings** or **Customize** options. These include features that may share information with apps such as a single setting to manage access to the Windows Location Platform.

  If the platform is turned on when a user runs a Windows Store app for the first time, Windows will ask the user whether the app may use location. Conversely, if the platform is turned off, apps cannot use the Windows Location Platform to access the user's location. At any time while using a Windows Store app, the user may easily enable or disable use of location.
- Windows Phone Kid's Corner allows parents and caregivers to pick the apps, games, videos, and music that kids can access, while protecting the adult's account from misuse.
- Microsoft works with mobile service providers and independent software companies to give families additional safety tools for mobile phones, such as content filtering, usage limits, and contact management.

POLICY CONSIDERATIONS

- As governments address risks associated with emerging technologies and online services, they should also ensure that innovation and technology adoption aren't stifled along the way. In addition, government and industry should collaborate to establish safety principles and help offer a more secure online environment for youth.
- Microsoft believes that the best way to protect children from inappropriate content is through the voluntary adoption of content controls, rather than through mandatory filtering or content ratings.
- Microsoft supports efforts by mobile providers to establish voluntary industry guidelines and best practices that address issues such as content classification, location-based services, and mobile commerce to help families make informed decisions about their safety.
- Because mobile devices can be effective tools for learning, Microsoft encourages governments to work with information and communications providers, online safety organizations, and school districts to promote safety curricula and address mobile safety.

Helpful Resources

Microsoft Safety & Security Center safety guidelines for the whole family
www.microsoft.com/security/family-safety

Kid's Corner for Windows Phone
aka.ms/Kids-Corner

The Family Online Safety Institute
www.fosi.org

Coalition of mobile providers in the United Kingdom promoting social responsibility in the mobile phone industry
www.mobilebroadbandgroup.co.uk/

February 2013

National Cyber Security Alliance

Key Points

- Governments, law enforcement agencies, the technology industry, and nonprofit organizations share the responsibility for helping make the Internet safer and more secure.
- For the past 10 years, the United States has designated October as National Cyber Security Awareness Month (NCSAM), a time to more formally encourage everyone to use the Internet more safely and responsibly.
- Microsoft is a founding member of the National Cyber Security Alliance (NCSA) and a key sponsor of NCSAM, which has expanded beyond the United States to include Canada and several members of the European Union. Microsoft encourages governments worldwide to adopt and promote October as Cyber Security Month as one way to help raise awareness of Internet risks among their people.

BACKGROUND

Microsoft and others in the technology industry have long maintained that helping to keep individuals and families safer online is a responsibility best shared among industry, government, law enforcement, and nonprofit organizations.

The National Cyber Security Alliance (NCSA) is a prime example of just such a successful partnership between the Department of Homeland Security, business, and nonprofit organizations. Microsoft, a founding member of the NCSA, has played a leadership role since its inception in 2001.

National Cyber Security Awareness Month (NCSAM) in the United States is a project of the NCSA—31 days dedicated to raising public awareness of online risks and informing individuals about ways they can help mitigate those risks. Microsoft contributions have included research, new consumer advice and guidance on key online safety and security issues, and participation in special forums and events.

October 2013 will mark the tenth anniversary of NCSAM and will welcome new signatories—Canada and eight members of the European Union. In 2012, those EU states—the Czech Republic, Luxembourg, Norway, Portugal, Romania, Slovenia, Spain, and the United Kingdom—piloted a European Cyber Security Month to great success.

Another significant NCSA contribution and example of public-private collaboration has been its signature consumer awareness and education campaign, STOP. THINK. CONNECT., launched in October 2010. Its simple message—to stop and think before going online—reminds people to exercise caution. The campaign, created by an unprecedented coalition of 30 private companies, nonprofit organizations, and government agencies, was the result of 16 months of research and testing.

MICROSOFT APPROACH

Microsoft takes a three-pronged approach to improving online safety:

- **Technology tools.** Microsoft offers a number of online safety tools, including Microsoft Security Essentials, a free antimalware program for consumers. Microsoft account holders can specify who can view their profiles, contact them, and post or view comments about their shared content. Microsoft Family Safety provides tools that help monitor and protect children online, and Xbox comes equipped with safety settings.

- **Education and guidance.** The Microsoft Safety & Security Center provides guidance for safer Internet use, including tips on how consumers can secure their computers, protect their online reputations, avoid online scams, secure mobile devices, and avoid, block, and report inappropriate behavior.

- **Building relationships.** Central to Microsoft's focus is engaging, through public policy, with governments around the world and with non-governmental organizations (NGOs) such as the NCSA.

POLICY CONSIDERATIONS

- Microsoft encourages governments and companies worldwide to invest jointly in Internet safety by supporting programs aimed at increasing public awareness and education. This could include adoption and support of October as Cyber Security Awareness Month, and STOP. THINK. CONNECT. as a central campaign to raise public awareness.

- Microsoft believes that cooperation among all stakeholders is the most effective means for reducing Internet risks, and supports balanced regulation that leaves room for innovation and flexibility in responding to those risks.

Helpful Resources

Microsoft Safety & Security Center
www.microsoft.com/security

Microsoft's online safety updates on Facebook
www.facebook.com/SaferOnline

National Cyber Security Alliance
www.staysafeonline.org

STOP. THINK. CONNECT. Online safety tips and guidance
www.stopthinkconnect.org

February 2013

Online Bullying

Key Points

- Online bullying 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 online bullying 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.

BACKGROUND

Bullying among youth has been a serious problem for many years, but technology now provides bullies with new ways to annoy their victims, giving rise to the phenomenon of online bullying, or cyberbullying. The Cyberbullying Research Center in the United States defines online bullying as "willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices." Online bullying can be thought of as a spectrum from meanness (including teasing) to bullying to cruelty, where someone intentionally sets out to harm another.

Youth who experience online bullying can suffer damaging mental health consequences, and according to the Cyberbullying Research Center,[1] "research reveals a link between cyberbullying and low self-esteem, family and academic problems, school violence, and delinquent behavior."

Estimates of the prevalence of online bullying 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 online bullying. A 2012 Microsoft survey in 25 countries found that 54 percent of children age 8 to 17 are concerned that they will be bullied online.

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

[1] *Cyberbullying Identification, Prevention, and Response* **www.cyberbullying.us/Cyberbullying_Identification_Prevention_Response_Fact_Sheet.pdf**

MICROSOFT APPROACH

- Microsoft enforces policies against abuse and harassment on its online services such as Xbox LIVE. Customers who misuse Microsoft services are subject to account termination. Serious incidents may be reported to law enforcement.

- Microsoft provides safety tools like Family Safety, which allows parents to monitor their children's Internet use and block unwanted contact.

- Microsoft works with governments, law enforcement agencies, educators, children's advocacy groups, and others worldwide to help create a safer online environment for children. It does this in part by monitoring online services for abuse and providing safety tools and education.

- Microsoft produces educational programs and materials for teachers, parents, and caregivers to teach young people how to stand up to online bullying.

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 legislation that provides a safe haven for companies that engage in online moderation of behavior and content by not increasing their liability for engaging in that moderation. Examples include Section 230 of the U.S. Communications Decency Act and the 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.

Helpful Resources

Microsoft Safety & Security Center materials to help protect young people from online risks
www.microsoft.com/security/resources/young-people.aspx

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

Cyberbullying Research Center
www.cyberbullying.us

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

A collection of online resources for addressing bullying in the United Kingdom
www.bullying.co.uk

Microsoft's free Family Safety software
aka.ms/Family-Safety

Online Reputation

Key Points

- Managing an online reputation is important—it can have a significant impact on the life of an individual in a number of ways, including employment prospects, relationships, and college admissions.
- Companies have an important role to play in helping their customers protect and cultivate their online reputations, by offering relevant education and guidance, and by creating content policies that help customers better manage their content.
- Governments should balance helping their citizens protect their online reputations with the right of free expression.

BACKGROUND

Worldwide, people are living more of their lives online than ever before. It's where many go to promote themselves, spend time with friends, and find employment, education, and even a spouse. A 2010 survey[1] found that 19 percent of the marriages in the United Kingdom and 17 percent in the United States originated online. Since 2010, nearly three quarters of U.S. job seekers use the Internet to find employment.

Research also shows that what appears about an individual online can have a significant impact on their prospects for employment and education. Microsoft research[2] in 2009 found that 70 percent of U.S. hiring managers and 41 percent of U.K. hiring managers had rejected a candidate because of information found online. A 2012 survey[3] found that 35 percent of admissions officers in the United States "discovered something that negatively impacted an applicant's chances of getting into the school."

Because a simple online search can reveal a great deal about an individual, there is increasing interest in online reputation, and in particular, one's *digital footprint*—the trail left by online activities such as blogging, posting comments or pictures, gaming, and social networking. While a positive digital footprint can enhance a person's employment and other prospects, a negative one caused by inappropriate photographs or rude comments left on online can damage those prospects.

In 2011, a Microsoft survey[4] of 5,000 adults and children in Canada, Germany, Ireland, Spain, and the United States found that 90 percent have done something to manage their online profile, but only 44 percent actively think about the long-term consequences their activities have on their online reputation.

[1] *Recent Trends: Online Dating*
cp.match.com/cppp/media/CMB_Study.pdf

[2] *Online Reputation in a Connected World, 2009*
www.microsoft.com/security/resources/research.aspx#reputation

[3] *Kaplan Test Prep's 2010 Survey of College Admissions Officers, 2012*
press.kaptest.com/research-and-surveys/kaplan-test-preps-2012-survey-of-college-admissions-officers

[4] *Online Reputation Management: Parents and Children 8-17, 2011*
www.microsoft.com/security/resources/research.aspx#onlinerep

MICROSOFT APPROACH

Education and guidance. The Microsoft Safety & Security Center offers guidance for appropriate Internet use, including tips on how consumers can protect their online reputations and avoid, block, and report inappropriate behavior.

Policies. The Microsoft Terms of Conduct do not allow customers to "upload, post, transmit, transfer, distribute, or facilitate distribution of any content" that "defames, defrauds, degrades, victimizes or intimidates an individual or group of individuals." Its Services Agreement states that "Microsoft may remove your content without asking you if we determine it's in violation of this agreement."

Technology tools. Microsoft offers features that help customers manage their digital footprint in its products and services. The Microsoft Personal Data Dashboard—a central location for personal information associated with selected Microsoft products and services—helps customers control how that information is displayed. Xbox LIVE enables customers to manage information about themselves.

POLICY CONSIDERATIONS

- Microsoft believes that governments must balance helping citizens protect their online reputations with the right of free expression.
- Companies can help their customers protect and cultivate their online reputations by offering relevant education and guidance and by creating policies that help them better manage their content.
- Microsoft supports legislation that provides a safe haven for companies that engage in online moderation of behavior and content by not increasing their liability for engaging in that moderation. Examples include Section 230 of the U.S. Communications Decency Act and the European Union Directive 2000/31/EC.

Helpful Resources

Microsoft Code of Conduct
aka.ms/code-of-conduct

Microsoft Services Agreement
aka.ms/services-agreement

Microsoft Personal Data Dashboard
aka.ms/dashboard

Microsoft Safety & Security Center:
Take charge of your online reputation
aka.ms/reputation

February 2013

Online Safety Education

Key Points

- While the Internet is an extraordinary tool for learning, it may also expose youth to certain risks, such as inappropriate content, online bullying, loss of privacy, or identity theft. 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 online safety, online security, and online ethics.
- Microsoft supports comprehensive online safety education as part of school curricula. Legislation requiring schools to implement online safety education should be broad enough to account for local variations in curricula.

BACKGROUND

The Internet is an extraordinary tool for enabling children to learn and explore the world around them, and many parents and educators recognize that being a good digital citizen is a prerequisite for their students. Access to the Internet offers children many benefits, but it may also expose them to certain risks, including potential exposure to inappropriate content, contact with bullies or strangers, and loss of privacy.

Teaching young people about digital citizenship 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.

Digital citizenship is usually defined as "the norms of behavior with regard to technology use." But digital citizenship is about more than social norms—it is about preparing young people for living and learning in a technology-rich society. Digital citizenship helps young people develop a sense of ownership and personal responsibility that, in turn, will help them make appropriate, ethical decisions in the online world.

Many schools do not teach or have access to a comprehensive online safety curriculum, even though safety experts and many online safety organizations identify education as an effective means of protecting children from online risks. A comprehensive online safety education curriculum needs to address:

- **Online safety.** Children are taught basic online safety habits and ways to avoid potential dangers. They learn to address issues and when to report problems to the appropriate adult authorities.
- **Online security.** Children are taught how to protect their accounts, identities, and privacy online. They learn the importance of strong and secret passwords and how to update their computers and devices to help protect them from viruses, spam, and phishing scams.
- **Online ethics.** Children are taught how good citizenship also applies in the online world and the risks of bullying, plagiarism, and the theft of money or identity. Children are given resources to deal with online bullying or harassment, and will understand the impact their postings or comments may have on others as well as the consequences of their actions.

MICROSOFT APPROACH

- Microsoft's approach to children's online safety includes technology tools; education and guidance; robust internal policies and practices for moderating content and addressing online abuses; and relationships with government, industry, law enforcement, and others to help create safer, more trusted computing experiences for all.

- The Microsoft Safety & Security Center 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 online bullying, safer social networking, using mobile devices more safely, responsible online gaming, and inappropriate online behavior.

POLICY CONSIDERATIONS

- **Integrating online safety education in the school curriculum.** A number of jurisdictions have required that online safety education be an integral part of school system efforts to achieve technological literacy for their students. Given the pervasiveness of technology in today's classroom, Microsoft believes that online safety education is an important component of any school curriculum.

- **Promoting online safety in the professional development of teachers.** Just as students need education about safer Internet use, teachers also need guidance and skills to stay ahead of the technology curve. As teachers receive training on how to more effectively use technology in the classroom, they also need to understand current Internet dangers, recognize when students may be subject to online risk, and guide them on conducting themselves ethically on the web.

- **Restricting online access is not a substitute for education.** Controlling 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 involve 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 from 26 Microsoft subsidiaries across Europe reaches more than 90,000 teachers, parents, and students with online safety education.

Helpful Resources

The Microsoft Safety & Security Center, with age-based guidelines for Internet use
www.microsoft.com/security

Microsoft Digital Citizenship in Action Toolkit
aka.ms/DC-Toolkit

European Commission Safer Internet Programme
aka.ms/EC-SaferInternet

National Cyber Security Alliance safety tools and materials
www.staysafeonline.org/teach-online-safety/

February 2013

Safer Online Gaming

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 technology 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 safer, more trusted computing experiences.
- Microsoft believes that online gaming concerns can be addressed with a combined approach of family education and involvement along with voluntary industry rating systems such as ESRB, PEGI, and CERO.

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 games on children. Some governments have responded to these concerns by restricting 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 the Entertainment Software Ratings Board (ESRB) ratings in the United States, the Pan European Game Information (PEGI) ratings in the European Union, the Computer Entertainment Rating Organization (CERO) in Japan, and others.

These widely recognized rating systems provide descriptive information about game content, which merchants are encouraged to display, and which parents can use as guides for buying video games. PEGI is used across more than 30 European countries, and a 2008 survey found that 93 percent of European consumers recognize PEGI labels. A 2011 survey found that 65 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 2011 found that 87 percent of U.S. merchants refused to sell games with a mature rating to a minor.

Regardless of the brand of entertainment products a family owns, or whether children play games, watch movies, video chat, or otherwise 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 decide if they want to use tools like family safety settings to help protect children by limiting Internet access, content, and the amount of time children spend on games.

MICROSOFT APPROACH

- **Technology tools.** Microsoft was the first to introduce ratings-based parental controls, called Family Settings, on the Xbox.
  - » Console Safety Settings for the Xbox 360 include the ability to enforce content ratings for games, movies, and television shows; set a pass code to restrict who can change Family Settings; and set limits on console play time using the family timer.
  - » Online Safety Settings for Xbox LIVE enable parents to create individual profiles for each child that are appropriate for their age and maturity. They can specify what activities children can participate in (such as multiplayer gaming, video chat, text or voice messaging), who they can communicate with, and who can see a child's profile or friends list.
- **Partnering with safety advocacy groups, industry, and government.** Microsoft, together with more than a dozen organizations—including the Boys & Girls Clubs of America and the National Center for Missing & 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.** Microsoft's 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 these resources. Microsoft provides these in the Microsoft Safety & Security Center, and the Get Game Smart website.
- **Internal policies and practices.** Microsoft's efforts to promote safety include developing company-wide policies, standards, and procedures for its products and services that connect with the Internet. The company enforces a code of conduct for users of its gaming services, and moderates content and interactions to address issues such as abuse, illegal activity, and inappropriate material. Many Microsoft services contain a Report Abuse link to Microsoft's **www.microsoft.com/reportabuse website**.

POLICY CONSIDERATIONS

- Microsoft supports a vibrant ecosystem that allows game developers and publishers to create products and content for customers of all ages. At the same time, the company wants 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 the combination of voluntary industry rating systems, family education, and parental involvement provides the best solutions for addressing concerns about gaming and other online entertainment.
- Microsoft supports many efforts to create and enforce laws against child exploitation. The company works with the International Centre for Missing & Exploited Children, INTERPOL, and other organizations to help governments strengthen and enforce laws to stop the possession and distribution of child pornography.

Helpful Resources

Safety resources for video games and online media
www.GetGameSmart.com

The Microsoft Safety & Security Center, with age-based guidelines for Internet use
www.microsoft.com/security

The International Centre for Missing & Exploited Children
www.icmec.org

Entertainment Software Ratings Board
www.esrb.org

Pan European Game Information
www.pegi.info

Computer Entertainment Rating Organization
www.cero.gr.jp

February 2013

Safer Social Networking

Key Points

- Social networks are very popular and offer enriching experiences, but they may include risks such as exposure to malicious software, potential loss of privacy, harassment, online bullying, and damage to reputation.
- Microsoft's approach to making social networks safer includes technology tools; education and guidance; internal policies and practices for moderating content and addressing online abuses; and partnerships with government, the technology industry, law enforcement, and others.
- Governments should continue to work with industry to encourage the benefits and mitigate the risks involved in online social networks by jointly establishing industry best practices and guidelines.

BACKGROUND

In recent years, the web has undergone a dramatic transformation from largely static webpages to a dynamic, interactive set of web-culture communities. There, people connect with their friends on Facebook or Pinterest or colleagues on LinkedIn, explore a virtual world like Second Life, post updates on Twitter, or play games on Xbox LIVE. Children play on their own social networks like Webkinz or Club Penguin.

The most popular social networks have hundreds of millions of members. Unfortunately, their popularity has also attracted criminals—hackers, spammers, identity thieves, and predators—who misuse the information people disclose to harass, bully, steal identities, and commit fraud. In addition, users of these services may reveal details about their lives that are more lasting and available to a wider audience than they may realize, with consequences for their reputations that they may not imagine. It is essential, therefore, for consumers to understand the risks and take appropriate steps to help protect themselves—their information, their privacy, and their reputations.

Social networking services may raise additional concerns for young people, particularly those under the usual required age of 13, who may use social networks designed for adults. It is important that young people (and their parents and guardians) understand that these sites may contain content inappropriate for children, and that many profiles can be viewed by anyone on the Internet. Registering children who are under the required age can violate the terms and conditions of these social sites. Furthermore, young people over 13 but under the age of majority who lie about their age may bypass protections offered for those under 18.

MICROSOFT APPROACH

Microsoft's approach to helping create safer, more trusted digital world includes:

- **Technology tools.** Microsoft offers a number of online safety tools, including Microsoft Security Essentials, a free antimalware program, and the Microsoft Personal Data Dashboard. The Dashboard offers a central location for personal information associated with selected Microsoft products and services to help customers control how their information is displayed.

  Also, Microsoft has built family safety features into many of its products, including Microsoft Family Safety in Windows 8, which helps monitor and protect children online, Kid's Corner on Windows Phone, and Console Safety Settings for Xbox and Xbox 360.

- **Education and guidance.** The Microsoft Safety & Security Center offers guidance on how to use social networks more safely, including those that are location-based, with specific advice for children and teens. Consumers can also find advice on maintaining and restoring their online reputation, suggestions for avoiding online scams, and tips on how to avoid, block, and report inappropriate behavior.

- **Internal policies and practices.** Microsoft enforces policies such as a code of conduct for users of Microsoft online services, and moderates content and interactions to address illegal activity, inappropriate material, and other abuse.

- **Partnerships.** Creating a safer online environment requires a holistic approach in which government leaders, law enforcement, technology providers, and non-governmental organizations (NGOs) all play vital roles. Central to Microsoft's efforts is engaging, through public policy, with governments around the world and with NGOs such as the National Cyber Security Alliance and the Family Online Safety Institute.

POLICY CONSIDERATIONS

- **Support public and private partnerships.** Social networking services should work with governments to help protect their customers by establishing industry best practices and guidance, such as the *Safer Social Networking Principles for the EU*.[1] This document "outlines the principles by which social network providers should be guided as they seek to help minimise potential harm to children and young people, and recommends a range of good practice approaches which can help achieve those principles." Microsoft, Facebook, Google, and 15 other social networking services collaborated to develop these principles.

- **Commission studies and fund research.** Research plays a critical role in identifying the factors that increase risks to people online and in dispelling myths that can lead to misplaced efforts to address them. Government funding is essential for both academic and industry research in these areas.

- **Online safety education in schools.** Microsoft believes that online safety curricula should become an integral part of schools' efforts to achieve technological literacy for their students, and should include modules that teach cyber safety, cyber security, and cyber ethics.

[1] **ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf**

Helpful Resources

The Microsoft Safety & Security Center safety guidance
www.microsoft.com/security

National Cyber Security Alliance
www.staysafeonline.org

The Family Online Safety Institute
www.fosi.org

STOP. THINK. CONNECT. Online safety tips and advice
www.stopthinkconnect.org

February 2013

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 malicious behavior and outright criminality.
- Everyone—consumers, parents, students, teachers, government, law enforcement, and business—has a role to play in helping to make the Internet a safer, more secure and trusted environment.
- Microsoft teamed with a broad coalition to launch STOP. THINK. CONNECT., a computing security and online safety campaign to raise awareness of Internet risks, and to promote strategies to help keep individuals and organizations safer online.

BACKGROUND

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

Today, thanks to heightened public awareness, many consumers know to use caution when clicking links in email, and can recognize dubious email notifications that they're "a winner," or have been selected to receive "a gift" from someone they've never even 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 individually.

In June 2009, the National Cyber Security Alliance (NCSA) and the Anti-Phishing Working Group (APWG) brought together a group of some 30 representatives from industry, business, and the nonprofit sector. Their goal: create a simple message that raises 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, that effort led by the NCSA and APWG expanded to include the Department of Homeland Security and other government agencies and departments.

Launched at the Seattle kickoff of National Cyber Security Awareness Month in October 2010, STOP. THINK. CONNECT. (STC) stands as a prime example of public-private cooperation. It is an important step toward building a culture of online safety, similar to public awareness efforts aimed at encouraging seat-belt use and preventing forest fires. In 2012, STC expanded internationally, and is taking shape in Canada, among the Organization of American States, and among several European Union Member States. Europe will also formally recognize October as Cyber Security Month in 2014.

MICROSOFT APPROACH

Microsoft takes a three-pronged approach to helping create safer, more trusted computing experiences.

- **Technology tools.** Microsoft offers a number of online safety tools, including Microsoft Security Essentials, a free antimalware program. Microsoft account holders can specify who can view their profiles, who can contact them, and who can post or view comments about their shared content on their Microsoft account. Microsoft Family Safety provides tools that help monitor and protect children online, and Xbox 360 comes equipped with Console Safety Settings.

- **Education and guidance.** The Microsoft Safety & Security Center provides guidance for safer Internet use, which includes tips on how consumers can secure their computers, protect their online reputations, avoid online scams, secure mobile devices, and avoid, block, and report inappropriate behavior.

- **Partnerships.** 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. Central to Microsoft's focus is engaging, through public policy, with governments around the world and with NGOs such as the National Cyber Security Alliance.

POLICY CONSIDERATIONS

- Microsoft encourages governments, both in the United States and internationally, to become involved in the STOP. THINK. CONNECT. coalition, and to promote and support the group's work.

- Microsoft believes cooperation among all stakeholders is the most effective means for reducing Internet threats, and it supports balanced regulation that leaves room for innovation and flexibility in responding to online risks.

Helpful Resources

STOP. THINK. CONNECT. Online safety tips and advice
www.stopthinkconnect.org

Microsoft Safety & Security Center
www.microsoft.com/security

Microsoft's online safety updates on Facebook
www.facebook.com/SaferOnline

Microsoft's online safety presence on Twitter
twitter.com/Safer_Online

February 2013

Accessibility

Key Points

- Accessible computer technology makes it easier for everyone to see, hear, and use their computers, and to personalize their computers to meet their own needs and preferences. For many people with impairments, accessibility is what makes computer use possible.
- Microsoft is committed to developing innovative accessibility solutions, and its efforts are concentrated in four key areas: accessibility in its products, leadership and awareness, innovation, and collaboration.
- Microsoft supports the work of governments to harmonize international standards and procurement approaches, promote effective compliance with accessibility standards, ensure technology neutrality, and support interoperability.

BACKGROUND

Information technology allows people to enrich their lives, increase commerce, and communicate around the globe. As technology plays an increasingly prominent role in life, it is vital that everyone, regardless of ability or age, be able to enjoy the benefits of the digital world.

Accessibility technology makes it easier for everyone to see, hear, and use computers, and to personalize them to meet their own needs and preferences. For many people with impairments, accessibility is what makes computer use possible. For people with low vision, default computer text may be too small to read, or they may not be able to see text at all. People with mobility impairments may not have use of their hands and arms that would enable them to use a standard computer. Accessible technology is particularly helpful for those who experience visual difficulties, pain in the hands or arms, hearing loss, or cognitive challenges.

Accessible computer technology is defined as:

- Accessibility options that let people personalize the computer display, mouse, keyboard, sound, and speech options.
- Assistive technology products such as screen readers and specialty keyboards, which provide access to individuals with vision, hearing, dexterity, language, or learning needs.
- Interoperability among assistive technology products, the operating system, and software programs.

Accessibility should be a fundamental consideration during product design, development, testing, and release.

MICROSOFT APPROACH

- **Accessibility.** Many Microsoft products feature options that promote accessibility and personalization.
  - » Windows 8 introduces touch-only devices, as well as touch-friendly updates to accessibility features, including Narrator and Magnifier. The Windows 8 Ease of Access Center lets individuals manage an array of accessibility options.
  - » Office 2013 provides integration with new Windows 8 accessibility features like Narrator and Magnifier, as well as tools like the Accessibility Checker for documents.

  - » Office 365 supports display modes that make the Word Web App and PowerPoint Web App accessible to screen readers. It also offers keyboard accessibility and high-contrast modes.

- **Leadership and awareness.** Microsoft engages in accessibility-related research and development projects, including large-scale nationwide studies, targeted usability studies, and one-on-one interviews. It raises awareness by publishing in-depth information about accessible technology for accessibility trainers, developers interested in accessibility, and other experts. The Microsoft Accessibility website and the Accessibility Update newsletter provide in-depth information about the accessibility of Microsoft products, including demos, tutorials, and guides. Accessibility and personalization information is available in 58 regions and 41 languages.

- **Innovation.** Microsoft promotes innovation in accessible technology through the Microsoft Accessibility Developer Center, which serves as a portal for guidance and technologies for the development of accessible apps. Many current Microsoft research and development projects are related to making PCs easier to use. Microsoft collaborates with leaders in the industry through such organizations as the Accessibility Interoperability Alliance and the Assistive Technology Industry Association.

- **Collaboration.** Microsoft collaborates with a wide range of organizations to help raise awareness of the importance of accessibility technology. Microsoft works with consumer advocacy organizations to better understand the challenges computer users with disabilities face, and partners with them to provide technology skills training for people with disabilities. Through valued relationships with the Partnership in Opportunities for Employment through Technology in the Americas, Unlimited Potential, and other such organizations, Microsoft is able to implement information technology skills training for people with disabilities.

POLICY CONSIDERATIONS

- **Develop and harmonize global standards.** Market-led accessibility standards that are globally harmonized and the procurement policies that reference them are the foundation of a robust ecosystem of interoperable technology.

- **Promote digital inclusion.** Governments should create policies and programs that advance digital inclusion for people with disabilities and older adults.

- **Ensure technology neutrality.** When governments consider accessibility standards, a guiding principle should be technology neutrality. Technology-neutral policies promote innovation, eliminate barriers to trade and market access, enhance competition, and prevent bias in government procurement.

- **Support interoperability.** Interoperability is a key feature of Microsoft's accessible technologies, and the company advocates for public policies that allow for a variety of complementary ways to achieve it. Governments should allow technology vendors and purchasers to use alternative solutions that best suit their needs.

Helpful Resources

Microsoft Accessibility website, with information about accessibility features in Microsoft products, as well as tutorials, demos, and guides
www.microsoft.com/enable

Assistive Technology Industry Association
www.atia.org