Microsoft

Privacy

Building Global Trust Online, 4th Edition

Microsoft Perspectives for Policymakers

Contents

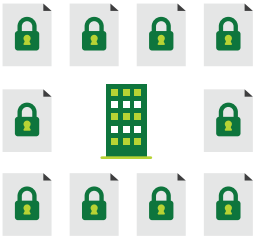
Our Commitment to Privacy

Microsoft is committed to earning customer trust by demonstrating accountability and an inherent respect for privacy. We must earn customer trust by being as transparent as possible about the people, policies, and processes we have in place to protect privacy.

Our approach to privacy[1]

We strive to use people's data responsibly, be transparent about our privacy practices & offer meaningful privacy choices

Microsoft conducts privacy reviews of new features, products, devices and services before release



The Microsoft Corporate Privacy Policy comprises 10 privacy principles to protect and appropriately use customer information

CONSUMERS

microsoft.com/yourprivacy provides guidance on how consumers can better protect their information online

ENTERPRISE

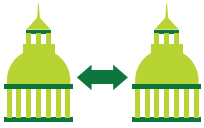
The Office 365 Trust Center, the Windows Azure Trust Center, and Dynamics CRM Online Trust Center and the Intune Trust Center describe how Microsoft cloud services help protect information privacy

The Microsoft Privacy Guidelines for Developing Software Products and Services is a public version of our internal privacy protection guidelines for our products and services

POLICY[2]

Microsoft works with governments, businesses, technology leaders, and civil society to:

Advise on legislative proposals



Help ensure interoperability of laws across jurisdictions

Develop responsible privacy practices

Strengthen self-regulatory mechanisms that support privacy and data protection

Read on to learn more about how Microsoft is innovating in privacy protection in support of consumers, enterprises, and government policy

[1]www.microsoft.com/en-us/twc/privacy/practices.aspx | [2]www.microsoft.com/en-us/twc/privacy/policy-activity.aspx

Privacy

Key Points

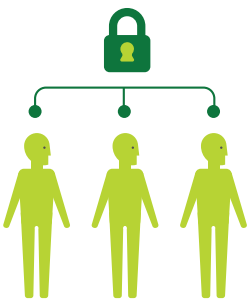
- Consumers expect strong privacy protections to be built into their products and services, and have high expectations about how companies collect, use, and store their information. Public trust depends on people knowing that their privacy will be protected and that their personal information will be 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 has more than 40 employees working full time on privacy, and several hundred others worldwide focused on privacy as part of their jobs.
- Microsoft supports privacy legislation that facilitates the free flow of information, builds trust with consumers, and encourages innovation. Because data increasingly flows across geopolitical borders, the company favors interoperability of privacy regulations, policies, and standards.

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 as well as widely publicized data breaches, threatens to erode public confidence in digital commerce and the Internet.

Consumers expect strong privacy protections 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 consumers will suffer.

Microsoft Approach

Microsoft has a longstanding commitment to privacy and takes steps to responsibly manage customer information, promote transparency, and offer meaningful privacy choices. The company's approach includes the following priorities:



PROMOTING 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.

PROTECTING 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 privacy principles and privacy statements provide clearly worded explanations of what information Microsoft collects, why, and how it is used. They also offer guidance on how consumers can manage the information they provide to Microsoft.

PROVIDING POLICY LEADERSHIP AND COLLABORATION

Microsoft works with governments, consumer advocates, businesses, and technology industry leaders to advise on legislative proposals, help create interoperable 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 privacy legislation. Microsoft also works with law enforcement agencies and consumer and advocacy organizations around the world to combat fraud, spam, spyware, and other threats to privacy online.

Policy Considerations

Policymakers in government and industry can help protect consumers' privacy and ensure that personal information is used appropriately by focusing on several priorities:

- **SUPPORT BALANCED, GLOBALLY INTEROPERABLE REGULATIONS AND STANDARDS** Privacy legislation should encourage innovation, facilitate the free flow of information, and help build trust with consumers. Because data exchanges are increasingly global, there should be greater interoperability of privacy regulations, policies, and standards worldwide.

- **ENCOURAGE INNOVATION AND NEW TECHNOLOGY** 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 globally interoperable.

- **SUPPORT A "DATA USE" MODEL FOR PRIVACY REGULATIONS** The way data is used, rather than how it is collected, might be a more effective premise for protecting data and meeting privacy obligations related to that data. Instead of relying strictly on notice and consent, policymakers should support a model that focuses on data use.

Baseline Privacy Legislation

Key Points

- In countries (like the United States) that have a patchwork of local and national privacy laws, policymakers should align these widely varied privacy requirements through clear, cohesive, and comprehensive national legislation.
- Microsoft has led the call for comprehensive federal 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 greater assurances about the security of their information.
- 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

Many countries have comprehensive privacy laws that govern how personal information is collected, used, and shared, and data protection authorities typically enforce those laws. In the United States, by contrast, privacy is governed through a combination of local and national laws that apply to specific industry sectors. This fragmented approach has led to a growing number of differing local and national laws, creating an environment of uncertainty for organizations and inconsistent protections for consumers.

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

Microsoft Approach

The longstanding commitment Microsoft has made to privacy includes principles, policies, and procedures for building privacy protections into its products and services—from development through deployment and operation. 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, as well as greater confidence in their online and offline transactions.

Key Points

commercial data in responsible ways.

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

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 it supported the development of the Asia-Pacific Economic Cooperation Privacy Framework. Further, Microsoft submitted comments in response to The White House Office of Science and Technology Policy's Request for Information regarding big data, and supported strengthening but adapting privacy law to enable the collection and use of data in a big data environment while preserving privacy, as well as adoption of baseline federal privacy law.

Policy Considerations

Policymakers can help provide consumers with greater control over the collection, use, and disclosure of their information by focusing on these priorities:

SUPPORT COMPREHENSIVE PRIVACY LEGISLATION Baseline federal privacy legislation should apply both online and offline, and it should include requirements for transparency, consumer control, and security. Legislation should create legal certainty by preempting state or local laws that are inconsistent with federal requirements. 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.

PROMOTE INDUSTRY SELF-REGULATION, BEST PRACTICES, AND CONSUMER EDUCATION 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.

REWARD SELF-REGULATION AND VOLUNTARY COMPLIANCE Privacy legislation should include safe harbors for companies that comply with 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.

Future Privacy Models

Key Points

- In light of the burden to consumers posed by the increasingly complex uses and reuses of their data, the current data protection model of notice and consent as the primary tool for data privacy should be reconsidered.
- Decision-makers should explore new models that retain the value of notice and consent where appropriate while shifting the focus of data protection to the use of information by accountable organizations.
- Microsoft encourages the adoption of privacy models based on use and organizational accountability, with corresponding legislation and enforcement capability that supports this approach.

Traditionally, data privacy in many parts of the world has been based upon the concepts outlined by the Fair Information Practice Principles, which rely upon protection mechanisms like notice and consent. This model typically requires an organization to give notice to individuals, often via a privacy statement, describing what information will be collected and how it will be used. Consumers give their consent by agreeing to the privacy statement or continuing to engage with the service. The organization commits not to use data in a manner inconsistent with the disclosures and consumers' consent.

However, in the modern information economy, the massive aggregation of digital information (sometimes referred to as big data) and increasing use of cloud computing are creating highly complicated flows of data that significantly strain the notice-and-consent model in at least four significant ways:

1. COMPLEX MANAGEMENT Choices regarding the collection of an individual's data and its use have become so numerous and detailed they are difficult for most individuals to interpret and manage.

2. CHANGING RELATIONSHIPS 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 with the proliferation of information sensors.

3. FUTURE USES OF DATA 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 enumerating potential uses at the time of the collection of data.

4. DATA PROCESSING AND ANALYSIS Increasingly large amounts of data will be created by entities (rather than amassed through collection alone) through analysis and data processing, further complicating the construct of notice and consent at the point of data collection.

There is a growing focus among privacy experts on the need for evolved data protection models, as the creation and use of data continues to grow. Under the current model, much of the responsibility for privacy protection rests with individuals, who are expected to read and make informed decisions based on the numerous lengthy, complex privacy statements and disclosures of online service providers. It is absolutely essential that organizations continue to be transparent about their data collection and use practices. However, if protection of personal privacy is to be meaningful, new models should be explored that retain the value of notice and consent in more appropriate ways while shifting the focus of data protection to the use of information by accountable organizations.

An additional challenge in our current data protection model relates to the specification of data use at the time of its collection. Today's technology-enabled data analysis and use are providing rich value-added scenarios and services to consumers, businesses, and society in general. However, there may be the potential to unlock additional value in data that was not contemplated at the time of collection.

Shifting the focus from a consent model to a data use model does not mean eliminating the concept of consent. Rather, a model that is more focused on use adds tools to the data protection arsenal, which can help cover gaps that are currently difficult to govern. Individual participation and consent remain critical parts of the privacy model and will become more important when individuals are confronted with data use or collection requests that are outside societal norms.

Microsoft Approach

Microsoft actively supports the idea that society must evolve its current data protection model and address its shortcomings by focusing less on the collection of data and more on the use of data. This does not mean collection limitation is unimportant—rather that it's not something societies can depend on as heavily for privacy protection in today's data-driven society.

Microsoft believes in the need for a greater focus on organizational accountability for responsible use of information, accomplished through formal assessment of the risks to individuals. The company recognizes the need for principles governing data usage that give individuals greater control over their data and provide greater transparency into how companies manage and use it.

Collectively, societies should focus on having the right privacy models in place that protect individuals' privacy needs while enabling accountable organizations to take advantage of the economic and social value of data use in a world of big data.

Policy Considerations

As societies work to evolve today's privacy models, policymakers should explore the following policy and regulatory considerations:

- **SUPPORT PRIVACY MODELS BASED ON DATA USE** Legislation should support privacy models that incorporate data use based on principles. A model based on data use can exist with an evolved set of Fair Information Practices as well as appropriate, relevant notice and consent in the privacy process. It also in no way diminishes the requirement that information be collected in a fair and lawful manner.

- **PROVIDE ADEQUATE ENFORCEMENT AND OVERSIGHT** Enforcement models should be resourced to tackle the oversight challenges that are associated with embracing greater organizational accountability for data use.

- **ENCOURAGE INNOVATION AND PUBLIC-PRIVATE COLLABORATION** 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 envision and identify the future of privacy models.

Microsoft Privacy Statements

Key Points

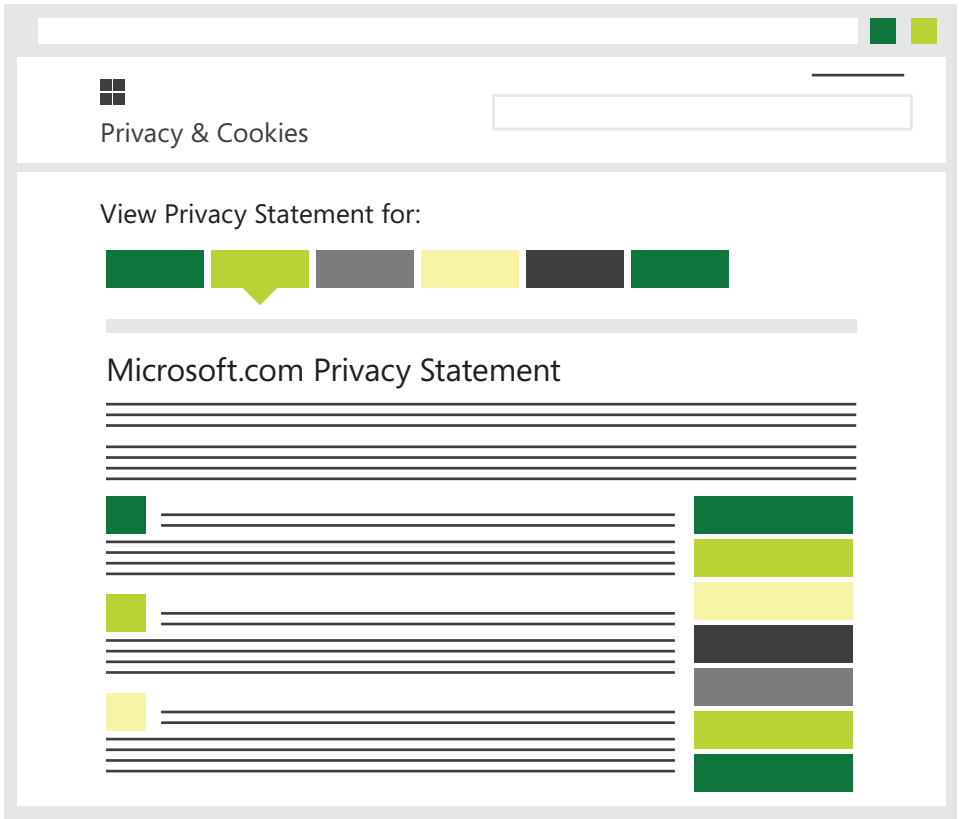
- Improvements to Microsoft online privacy statements enhance their design and functionality to more effectively layer important information and make that information easier to locate and use.
- Migration to the new privacy statement format will be gradual but steady. Bing and Microsoft.com were the 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 uphold its privacy policies and practices. There are no material changes to Microsoft data collection and use practices as a result of the redesign.

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 meaningful 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 statement. 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 in the following figure) being the first to adopt the new format, followed by Xbox in October 2012, and MSN in December 2013.



Microsoft Approach

By providing a new format and design of its privacy statements, Microsoft aims to accomplish the following:

IMPROVED CONSISTENCY AND AVAILABILITY Enhance functionality by enabling more effective layering of important information and creating a consistently accessible structure across many Microsoft products.

EASE OF USE 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.

BETTER ORGANIZATION Include clearly defined subsections specific to different types of data collection and use, such as advertising and cookies, how information is collected and used, 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 uphold its privacy policies and practices. There are no material changes to Microsoft data collection and use practices resulting from this redesign.

Policy Considerations

Government and industry policymakers alike can help ensure that privacy notices are transparent, discoverable, and easy to understand by focusing on the following priorities:

- **PROVIDE FLEXIBLE LEGISLATION THAT ALLOWS FOR INNOVATION** 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 customer data not only today, but in the years to come.

- **AVOID "ONE-SIZE-FITS-ALL" MANDATES** Although 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.

- **SUPPORT ADAPTABILITY IN INDUSTRY POLICIES AND PRACTICES** 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.

Privacy Accountability

Key Points

- Under the principle of accountability for data privacy, an organization is responsible for understanding the risks that are inherent in processing individuals' 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 manage personal data. Each Microsoft business unit is responsible for adopting procedures to help uphold the company's commitment to protecting personal data.
- Microsoft supports an accountability-based approach to data use and data transfers across international borders. Under an accountability regime, data could be used for activities based on accepted societal norms and be transferred across borders without restriction as long as the data exporter remains accountable for protecting the data regardless of its geographic location.

Accountability is a long-established principle of privacy and data protection. It was first set 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 (EU) and EU member states and is outlined more explicitly in the Canadian Privacy Law (PIPEDA) and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.

Accountability requires companies that use and store data to analyze and understand the related privacy risks for individuals, and take necessary and appropriate steps to mitigate those risks. Accountability calls upon organizations to implement programs that align with data protection principles, take responsibility for the safe and appropriate use and storage of data (regardless of its location), and be able to explain how its 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 usable data exists than ever before. This new world of available, interconnected data requires meaningful privacy safeguards that can address the size of the challenge.

Accountability for data privacy has experienced a recent resurgence in privacy policy circles worldwide. The privacy community is evaluating how to evolve current privacy models and principles to achieve meaningful privacy protections in a world of big data. The widespread adoption of a principle of accountability offers many potential benefits; it can help facilitate the flow of data across international borders and support cloud computing by requiring that businesses take responsibility for the management of information, regardless of how it is collected or used.

Microsoft Approach

A key Microsoft privacy principle is that of accountability in handling its customers' personal data within the company and with its vendors. Each Microsoft business unit is accountable for implementing procedures to help safeguard data and for assigning responsibilities for privacy protection to specific staff members.

Microsoft works with policymakers and other stakeholders to consider how organizations can implement and advance accountability, and whether (and how) third-party accountability agents and other validation programs might play an appropriate and proportionate role in this evolving paradigm.

Policy Considerations

Policymakers and other stakeholders can support the principle of accountability for data privacy by focusing on several priorities:

- **SUPPORT AN ACCOUNTABILITY-BASED APPROACH TO DATA PRIVACY** Such an approach would hold the data collector accountable for its uses and transfers of personal information. An accountable organization incorporates privacy protections in its technology systems and data management processes. The organization provides clear privacy notices that state what steps are being taken to minimize privacy risks and offers appropriate choices for individuals regarding data collection and usage.

- **LIMIT RESTRICTIONS ON INTERNATIONAL DATA TRANSFER** An accountability regime must permit 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.

- **SUPPORT INNOVATION AND FLEXIBILITY WHILE PROTECTING CONSUMER PRIVACY** Policymakers and other stakeholders should carefully consider how the accountability model might work within legal regimes so as to better protect consumer privacy—and permit organizations to use data in responsible and flexible ways to support innovation.

- **AVOID IMPOSING DIFFICULT VALIDATION REQUIREMENTS** Accountability should not require burdensome external validation mechanisms. For instance, imposing third-party audits or certification schemes can be onerous, expensive, and disproportionate to the potential privacy risks.

Privacy by Design at Microsoft

Key Points

- The longstanding Microsoft commitment to privacy includes tools, technologies, people, processes, and procedures for embedding privacy protections in its products and services—from development through deployment and operation.
- Microsoft employs more than 40 people who work full time on privacy, and hundreds of other employees worldwide focus on privacy as part of their jobs.
- Microsoft supports privacy legislation initiatives that facilitate the free flow of information, build trust, and encourage innovation. Because data increasingly flows across geopolitical borders, the company favors greater interoperability of privacy regulations, policies, and standards worldwide.

Privacy by Design has become a popular term in the privacy community, but it means different things to different people. At Microsoft, Privacy by Design describes not only how the company builds products, but also how it operates its services and conducts business as an accountable technology leader. Microsoft believes that all companies that operate online should adopt privacy practices that build trust with the customers who use their products and services.

Microsoft addresses Privacy by Design with principles, policies, and procedures to establish privacy-specific design objectives for its software products and online services at the outset of development. The company continues to address privacy and data security considerations throughout the product life cycle and uses internal processes to track compliance.

Microsoft has a longstanding commitment to privacy. More than a decade ago, it was one of the first companies to appoint a chief privacy officer. Microsoft currently employs more than 40 people who focus on privacy full time, and hundreds of others across the company and around the world support privacy as part of their jobs. The company's commitment to privacy begins with the Microsoft Privacy Principles, which address accountability, notice, collection, choice and consent, use and retention, disclosure of onward transfer, quality assurance, access, enhanced security, and monitoring and enforcement.

Microsoft Approach

Microsoft implements its commitment to privacy in many ways, including the following:

EMAIL AND FILE PRIVACY Microsoft does not scan the contents of Office 365 or Outlook.com customers' email or OneDrive documents for the purpose of serving ads.

TRUST CENTERS The Windows Office 365 Trust Center, the Windows Azure Trust Center, Windows Intune Trust Center, and the Dynamics CRM Online Trust Center describe how Microsoft cloud services help protect information privacy and security.

DO NOT TRACK People are worried about online tracking and want to protect their privacy, which is why Do Not Track (DNT) is enabled in Internet Explorer 11. Customers can turn DNT off at any time.

WINDOWS 8.1 The Windows 8.1 operating system was built with privacy in mind. It provides customers with the broad range of controls they need to make appropriate privacy choices.

KINECT AND XBOX ONE Microsoft created Kinect and Xbox One from the ground up with built-in privacy controls and safeguards that put customers in charge of their entertainment experiences and allow them to customize how their personal information or data is, or is not, shared.

Policy Considerations

Policymakers can help further Privacy by Design efforts to address privacy and data security throughout the industry by promoting several important principles:

- **ENCOURAGE INDUSTRY-WIDE ADOPTION OF PRIVACY BY DESIGN** Encourage companies to embrace these concepts by adopting guidelines and processes to build privacy into products and services through design, development, and deployment.

- **ENSURE INNOVATIVE, TECHNOLOGY-NEUTRAL PROCESSES** Privacy by Design principles are fundamental and can be supplemented by consumer education, self-regulation, and carefully crafted legislation. Such legislation should provide incentives to adopt Privacy by Design processes that are technology-neutral and do not stifle product development and innovation.

- **DEVELOP GLOBALLY INTEROPERABLE BASELINE PRIVACY LEGISLATION AND STANDARDS** Privacy initiatives should facilitate the free flow of information, build trust, and encourage innovation. Because data flow is global, companies should strive to create greater interoperability of privacy regulations, policies, and standards on a worldwide basis.

Privacy in the Cloud

Key Points

- The advances and increased adoption of cloud computing raise important policy considerations, including shared data storage, geographic location of data, transparency, access, and security.
- Microsoft has been providing cloud services for a number of years; it has consistently worked to understand customers' concerns and requirements to develop solutions that include robust privacy and security features.
- Microsoft prioritizes the privacy, security, and compliance needs of its customers, and its enterprise cloud services— including Office 365, Microsoft Dynamics CRM Online, Windows Intune, and Windows Azure— incorporate industry-leading privacy protection, security safeguards, and regulatory compliance features.

For organizations throughout the world—including governments, nonprofits, and businesses— cloud computing has become a key part of their ongoing information technology (IT) strategy. Cloud services give organizations of all sizes access to virtually unlimited data storage while freeing them from the need to purchase, maintain, and update their own networks and computer systems. However, as organizations continue to take advantage of the benefits of cloud services, they must consider two main things: how to secure their data in the cloud and how to protect their private information.

The following are some of the specific concerns cloud service providers must consider:

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 in order 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 providing contractual commitments, 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 example, 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.

Key Points

- 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.

Microsoft Approach

Microsoft has been providing cloud services for a number of years and has consistently worked to understand customers' concerns and requirements to develop solutions that include robust privacy and security features. Microsoft prioritizes the privacy, security, and compliance needs of its customers and provides enterprise cloud services, including Office 365, Microsoft Dynamics CRM Online, Windows Intune, and Windows Azure. These services incorporate industry-leading privacy protection, security safeguards, and regulatory compliance features.

Microsoft works closely with regulators and has incorporated their feedback into its approach, enabling customers to use cloud services with confidence. The Microsoft approach to cloud privacy encompasses the following priorities.

MAINTAIN A HIGH LEVEL OF DATA SECURITY Office 365, Microsoft Dynamics CRM Online, Windows Azure, and Windows Intune meet or exceed ISO 27001, a security certification that sets out a series of physical, process, and management controls. Refer to each service's Trust Center for a link to their ISO certification.

USE CUSTOMER DATA ONLY TO PROVIDE THE SERVICE—NOT FOR ADVERTISING Microsoft believes that the data that enterprise customers host in cloud services belongs to those customers, and should not be used by a cloud provider for purposes other than to provide the customers' service. This concept is in the company's enterprise cloud service agreements and is explained on its Trust Center websites. Customer data is defined as "all the data, including all text, sound, software, or image files that a customer provides, or are provided on the customers' behalf, to Microsoft through use of the Online Services." Microsoft does not use customer data for purposes unrelated to providing the service, such as advertising. Additionally, each service has establisheda set of standards for storing and backing up data, and for securely deleting data upon request from the customer.

DESIGN SOLUTIONS TO MEET CUSTOMER COMPLIANCE NEEDS Microsoft invests in developing and improving compliance processes that enable it to meet a wide range of standards efficiently and effectively. For example, Microsoft convened experts from the academic, public, and private sector in a joint effort that resulted in crafting a Business Associate Agreement that was satisfactory for a variety of regulated entities, including universities and health systems. Likewise, Microsoft has collaborated with financial services customers and banking regulators to develop compliance solutions, which will satisfy certain access and oversight requirements that the customer alone could not satisfy.

SUPPORT THE EUROPEAN UNION MODEL CLAUSES EU data protection law prohibits transfer of EU customer personal data to countries outside the European Economic Area (EEA) unless there are adequate protections for that data. Microsoft provides a contractual commitment to the processes and protections in its online services in the form of a data processing agreement, including contractual terms approved by the EU, known as the Standard Contractual Clauses (Model Clauses). Microsoft customers can take comfort that, by signing EU Model Clauses with Microsoft to assure adequacy for EU data protection law, they have the strongest commitment available in the industry regarding data transferred from within the EU. The European Union's 28

data protection authorities, acting through their "Article 29 Working Party," have determined that the contractual privacy protections Microsoft offers to its enterprise cloud customers meet the current existing EU standards for international transfers of data. Microsoft is the first and only cloud provider to receive this type of approval. Europe's privacyregulators have said, in effect, that personal data stored in Microsoft's enterprise cloud is subject to Europe's rigorous privacy standards no matter where that data is located. This recognition applies to Microsoft's enterprise cloud services – in particular, Microsoft Azure, Office 365, Microsoft Dynamics CRM and Windows Intune. Microsoft also abides by the U.S.-EU Safe Harbor Framework and the U.S.-Swiss Safe Harbor Framework as set forth by the U.S Department of Commerce regarding the collection, use, and retention of data from the EEA and Switzerland.

SEEK INDEPENDENT THIRD-PARTY AUDIT AND CERTIFICATION Microsoft obtains independent third-party audits, such as SSAE16 SOC1 and SOC2, and certifications, such as ISO 27001, so users can trust that its services are designed and operated with stringent safeguards.

MAINTAIN TRANSPARENCY Through its Trust Centers for Office 365, Microsoft Dynamics CRM Online, Windows Intune, and Windows Azure, Microsoft provides easy-to-understand information about where customer data is stored, who can access it, and the identity of any sub-contractors that may handle personal data. Customers can sign up to receive notifications about changes to geographic data flow information. Regarding requests for customer data from law enforcement or other governmental entities, Microsoft is firm in its commitment to protect customer data. It provides data only for lawful requests for specific sets of data. The company does not disclose customer data to a third party (including law enforcement, other government entity, or civil litigant) except as customers direct or as required by law. If a third party contacts Microsoft with a demand for customer data, the company tries to redirect the third party to request it directly from customer. If compelled to disclose customer data to a third party, Microsoft promptly notifies the customer and provides a copy of the demand, unless legally prohibited from doing so.

Policy Considerations

Policymakers can help boost consumer confidence and address concerns over data security and privacy in cloud computing by focusing on several priorities:

- **CREATE INTEROPERABLE DATA SECURITY AND PRIVACY LAWS ACROSS JURISDICTIONS** 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.

- **SUPPORT TECHNOLOGICAL INNOVATION AND INDUSTRY COLLABORATION** As governments develop policies that address the privacy and security concerns associated with 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.

Resources

GENERAL

Overview of Microsoft privacy policies and initiatives: **www.microsoft.com/privacy**

Microsoft Privacy Practices: **www.microsoft.com/privacy/principles.aspx**

Privacy Guidelines for Developing Software Products and Services (PDF, 1.16 MB):

aka.ms/privacy-guidelines

Privacy settings for Microsoft technologies: **www.microsoft.com/yourprivacy**

Microsoft Trustworthy Computing: **www.microsoft.com/twc**

FUTURE PRIVACY MODELS

Perspectives on evolving privacy models:

www.microsoft.com/en-us/twc/privacy/models.aspx

Microsoft Perspectives on Evolving Privacy Models (PDF, 126 KB):

download.microsoft.com/download/1/5/4/
154763A0-80F8-41C8-BE52-80E284A0FBA9/Evolving-Privacy-Models.pdf

MICROSOFT PRIVACY STATEMENTS

Microsoft Privacy Statement: **aka.ms/privacy-statement**

MICROSOFT CLOUD RESOURCES

Cloud Privacy: **www.microsoft.com/en-us/twc/privacy/cloud-privacy.aspx**

TRUST CENTERS

Microsoft Dynamics CRM Trust Center:

www.microsoft.com/en-us/dynamics/crm-trust-center.aspx

Office 365 Trust Center: **www.trust.office365.com**

Windows Azure Trust Center: **www.windowsazure.com/en-us/support/trust-center/**

Windows Intune Trust Center: **www.microsoft.com/en-us/WindowsIntuneTrust**

PRIVACY ACCOUNTABILITY

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

Information Policy Centre - Accountability-related papers: **aka.ms/accountability-papers**

PRIVACY BY DESIGN AT MICROSOFT

Privacy by Design: **www.microsoft.com/privacy/bydesign.aspx**

PRIVACY IN THE CLOUD

Cloud Privacy at Microsoft: **www.microsoft.com/privacy/cloudcomputing.aspx**

Privacy in Microsoft advertising: **choice.microsoft.com**

Protecting Data and Privacy in the Cloud (PDF, 372 KB):

go.microsoft.com/?linkid=9694913

Law Enforcement Requests:

www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/

Brad Smith Blog Post - Responding to government legal demands for customer data:

blogs.technet.com/b/microsoft_on_the_issues/archive/2013/07/16/responding-to-government-legal-demands-for-customer-data.aspx

GLOBAL PARTNERSHIPS AND INITIATIVES

Children's Online Privacy Protection Act:

www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

European Union Data Protection Directive:

ec.europa.eu/justice/data-protection/index_en.htm

Asia-Pacific Economic Cooperation Privacy Framework:

publications.apec.org/publication-detail.php?pub_id=390

Organization for Economic Co-operation and Development (OECD): **www.oecd.org/**

US – European Union Safe Harbor Framework:

www.export.gov/safeharbor/eu/eg_main_018365.asp

US – Switzerland Safe Harbor Framework: **www.export.gov/safeharbor/swiss/index.asp**