Microsoft

How Microsoft is taking Privacy by Design to Work

Alan Chan
National Technology Officer
Microsoft Hong Kong
7 May 2015

Agenda

- Introducing the New Microsoft
- Microsoft privacy principle
- Protecting privacy in Microsoft
- Implementing Privacy By Design in the Cloud

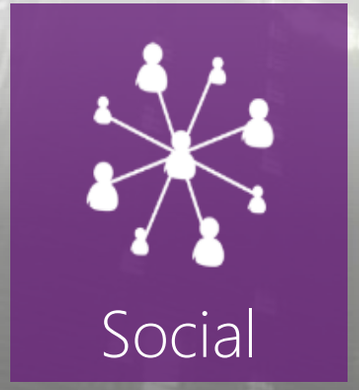
Introducing the new Microsoft

Technology Megatrends

Shift to a Data Driven Economy

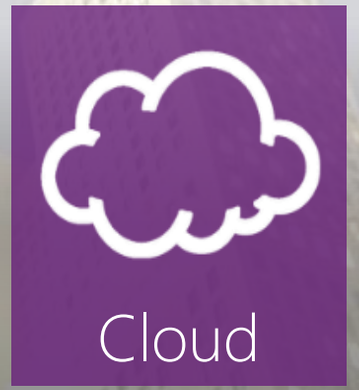
Mobility

By **2016**, **smartphones** and **tablets** in service by **2.7 billion** Asians.



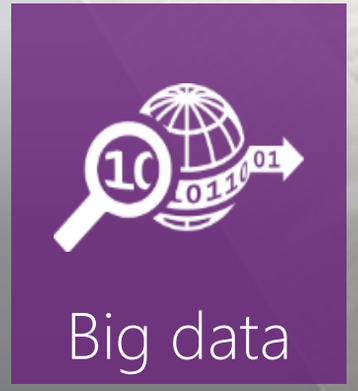
Social

Millennials will make up **59%** of the **Asian workforce** by **2025**



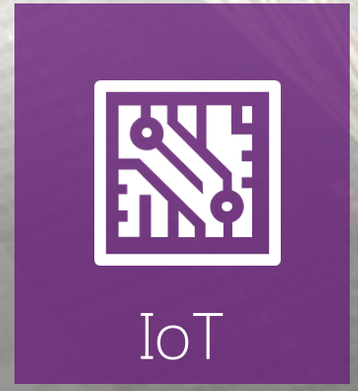
Cloud

50% of organizations are either using or investigating **cloud computing solutions in Asia by 2014**



Big data

Digital content will grow from less than **0.5ZB in 2013**, **up 90%** rocketing toward **4.8ZB by 2017**



IoT

IoT Devices will grow to **50B by 2020**, **with a market potential of 10 Trillion devices**

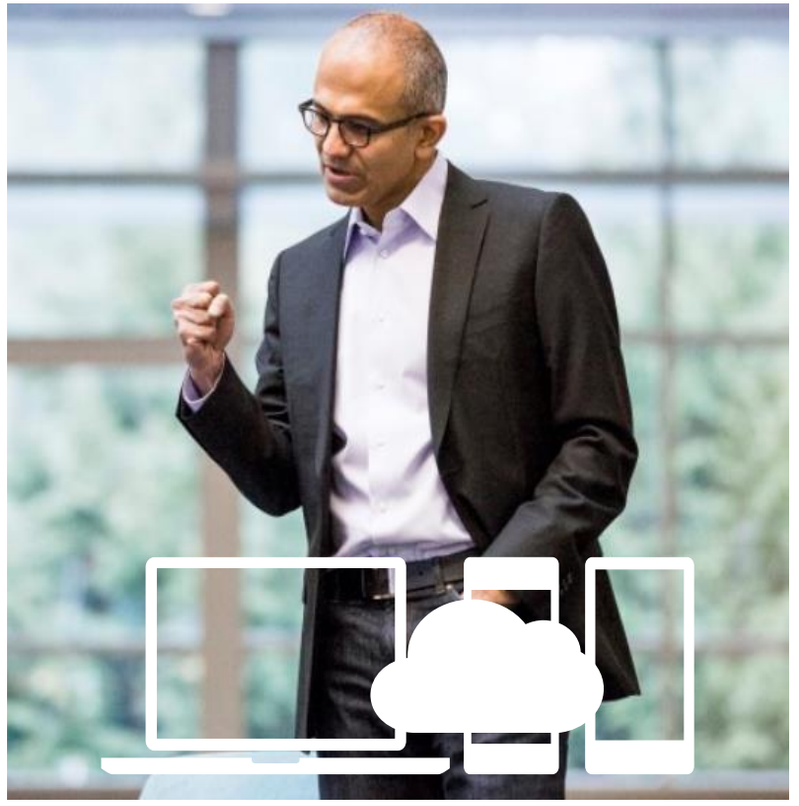
1 ZB = 10^{21}bytes = = 1 billion terabytes

Big/bold ambitions

A PC on every desk and in every home

Empowering everyone

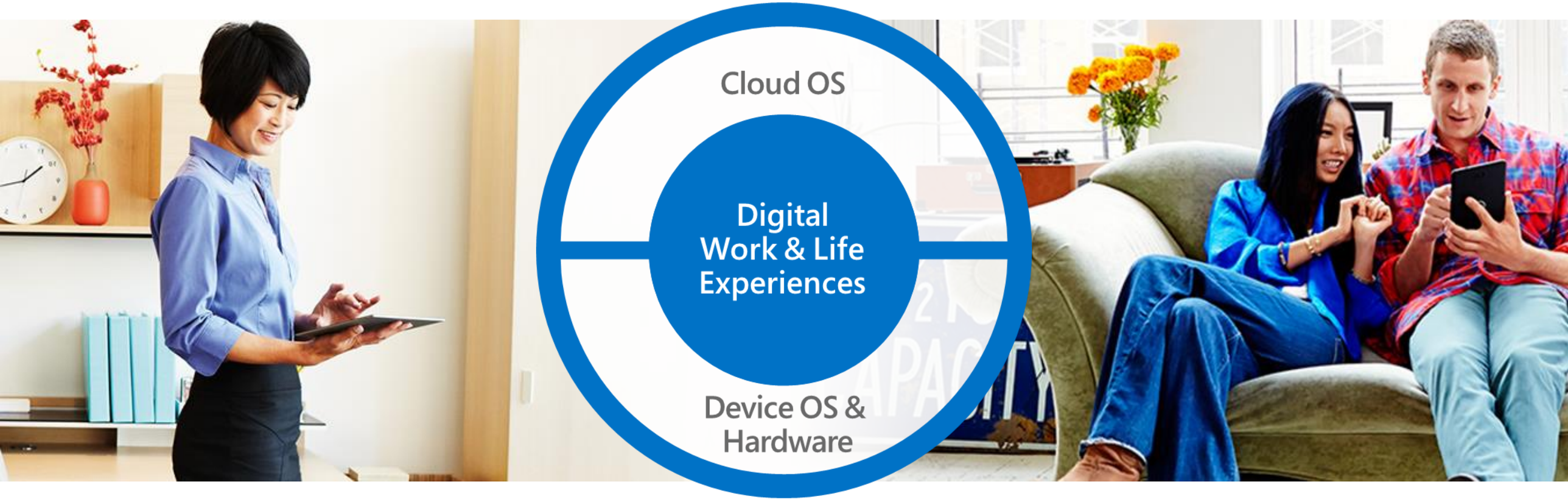
Realizing people's unlimited potential



Productivity and platform

Reinvent productivity to empower every person and every organization to do more

Microsoft – *Our Future --*



We Are the Productivity and Platform Company
for the Mobile-first and Cloud-first World!

Microsoft Privacy Principles

Privacy remains Microsoft's #1 priority

Microsoft: Recognizes that trust is critical to customer relationships and the long-term success of the brand

Customers: Know that their privacy/personal information is protected

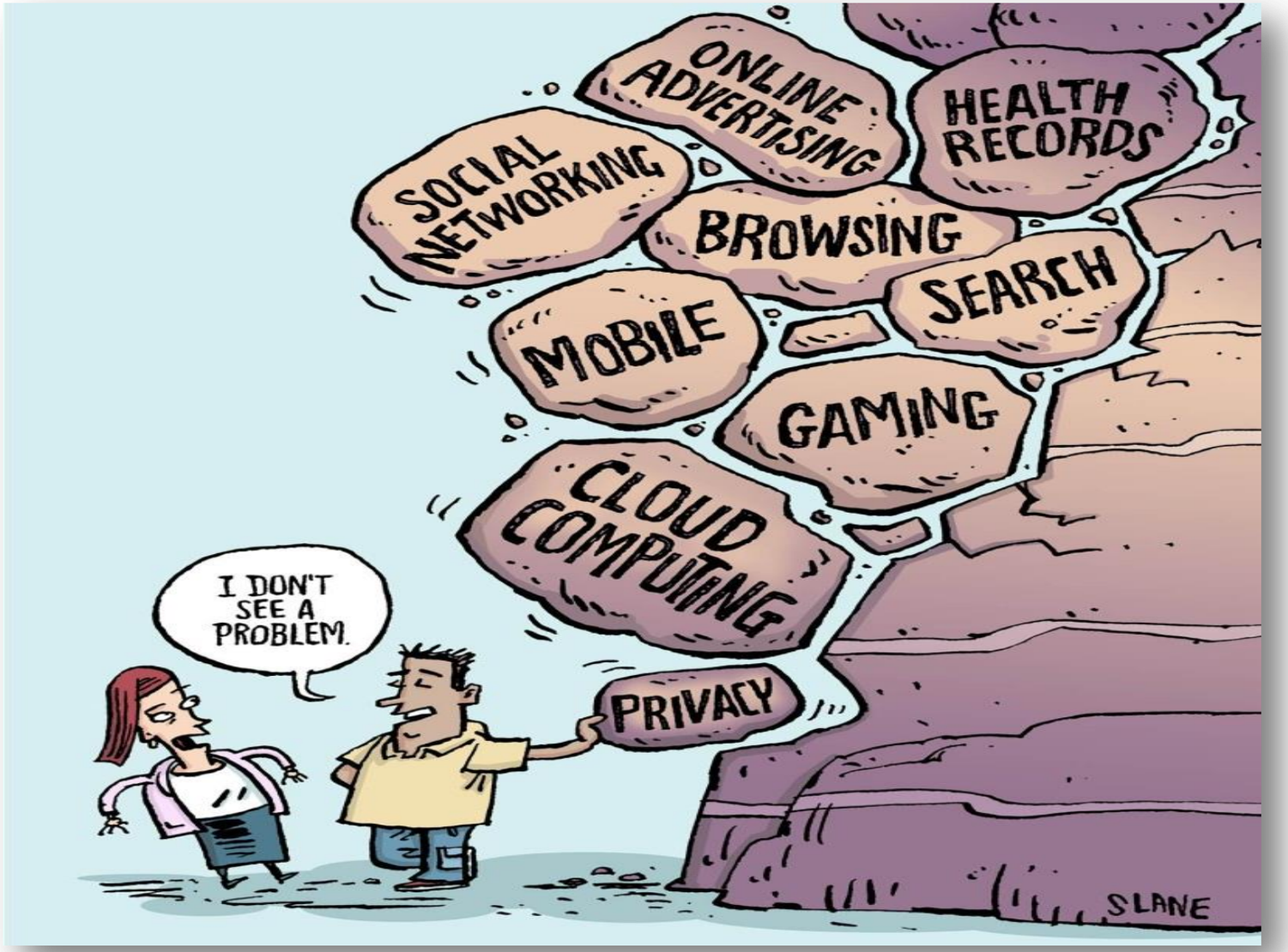
Partners: Influence customer trust as they communicate on Microsoft's behalf

Sales and Marketing: Execute under Microsoft's privacy practices

Comprehensive privacy program in place 10+ years

40+ full-time privacy professionals. Several hundred others with privacy-related responsibilities

No Big Deal ? It's everyone's business !



Microsoft's Privacy Policy

10 Privacy Principles

- Accountability
- Disclosure or Onward Transfer
- Notice
- Quality
- Collection
- Access
- Choice and Consent
- Security
- Use and Retention
- Monitoring and Enforcement

Protecting Privacy in Microsoft

Privacy in action for sales & marketing

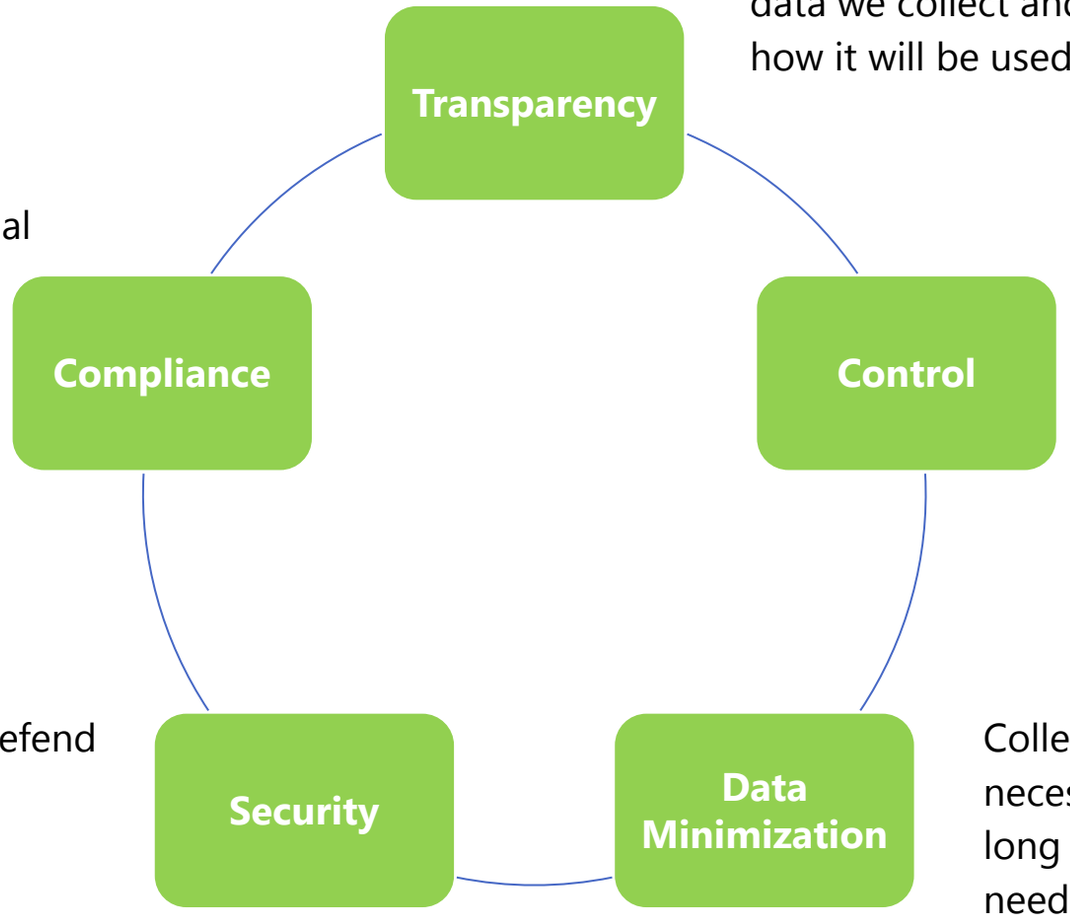
Tell customers what data we collect and how it will be used.

Empower users to control collection, use, & distribution of their personal information.

Collect only data that's necessary and retain only as long as there's a legitimate need.

Establish protective measures to defend against hostile acts or influences. Provide assurance of defense.

Ensure our data practices comply with Federal, State, and International laws – we must be compliant to avoid penalties.



Examples of protecting privacy in action

- Transactional vs. Promotional Emails
- Request Customer or Partner List
- Supplier Security & Privacy Assurance
- Sensitive Data storage

Implementing Privacy By Design in the Cloud

The Microsoft Trusted Cloud

200+ cloud services,

1+ million servers,

$15B+ infrastructure investment

1 billion customers,

20 million businesses,

90 countries worldwide[1]

57%
of Fortune 500[4]
10,000 new subscribers per week[2]
Microsoft Azure

3.5 million
active users[4]
Microsoft Dynamics CRM Online

300+ million
users per month[5]
skype

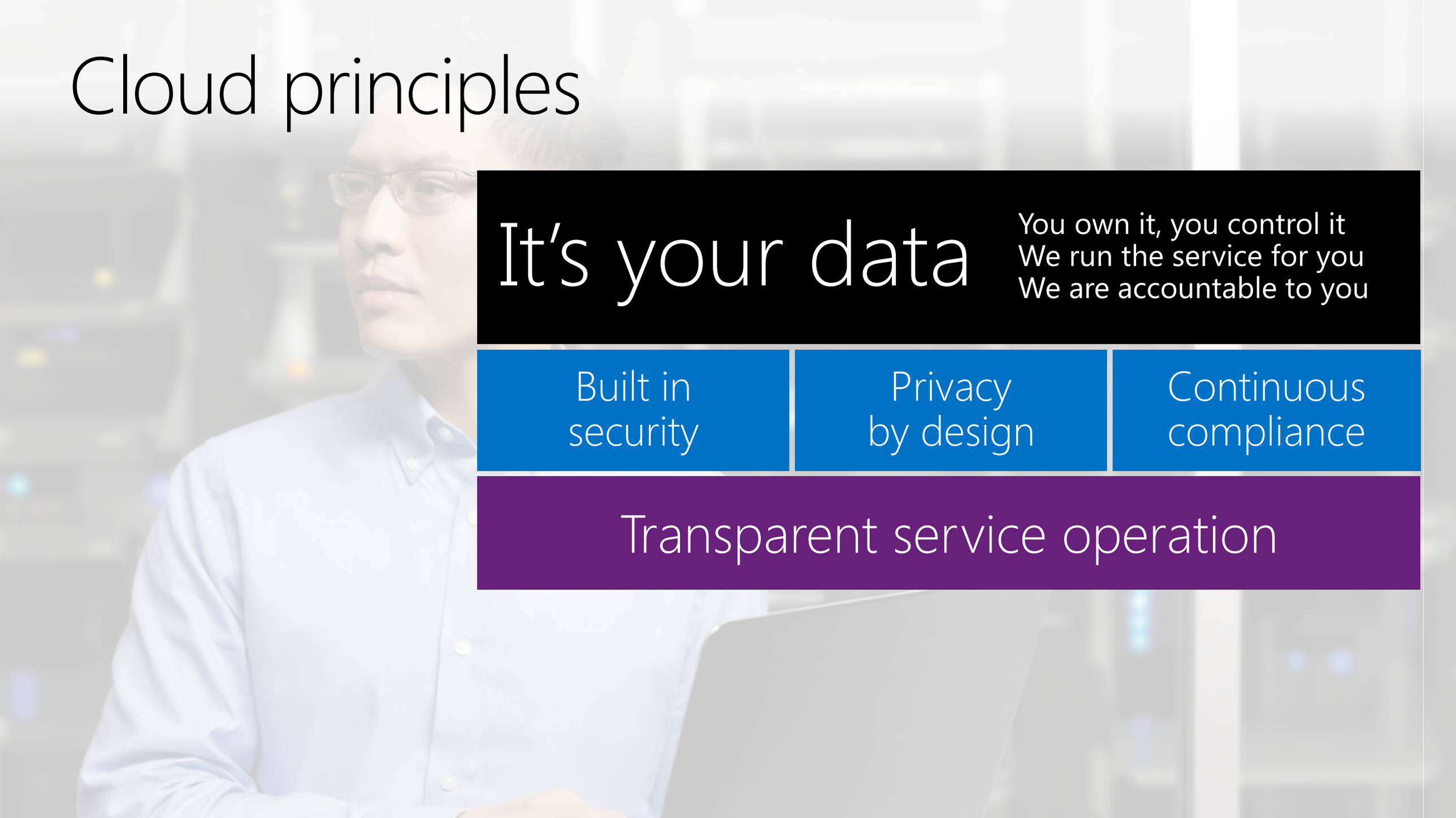
5.5+ billion
worldwide queries each month[3]
bing

1.2 billion
worldwide users[2]
Office 365

48 million
members in 57 countries[4]
XBOX

450+ million
unique users each month[6]
msn

Cloud principles



It's your data

You own it, you control it
We run the service for you
We are accountable to you

Built in security

Privacy by design

Continuous compliance

Transparent service operation

Privacy & Control in Commercial Cloud

Microsoft makes our commitment to the privacy of our customers a priority with independently audited policies and practices that include restricting the mining of Customer Data for advertising or similar commercial purposes.

Security without compromising experience

Techniques for securing the data should be specific to the type of cloud service

IaaS

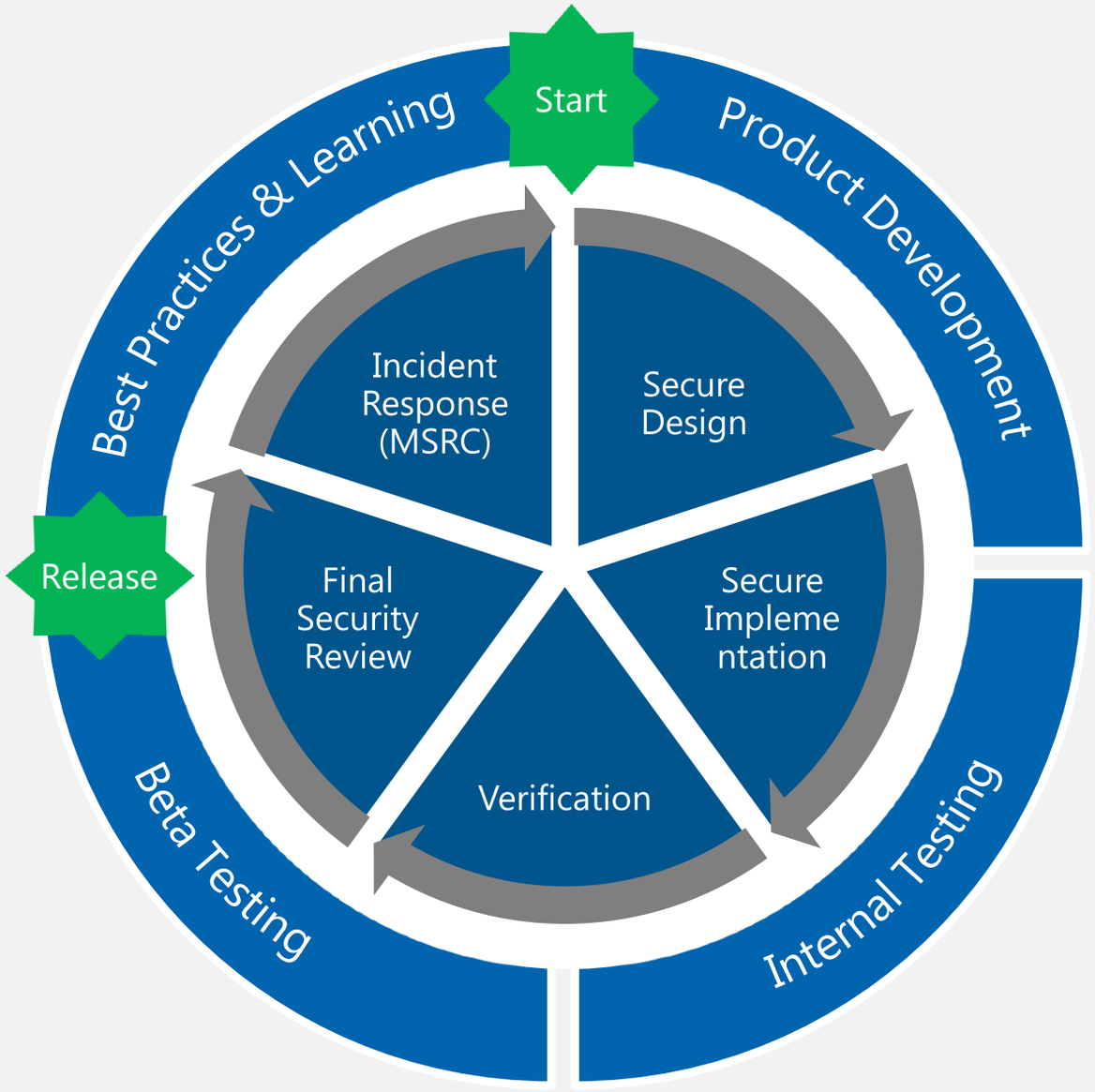
PaaS

SaaS

	IaaS	PaaS	SaaS
Applications			■
Data			■
Runtime		■	■
Middleware		■	■
O/S		■	■
Virtualization	■	■	■
Servers	■	■	■
Storage	■	■	■
Networking	■	■	■

■ Service Provider security responsibility

The Microsoft Security Development Lifecycle



Goals

Protect Microsoft customers by

- Reducing the **number** of vulnerabilities
- Reducing the **severity** of vulnerabilities

Key Principles

Secure by design

- Eliminate security problems early

Prescriptive yet practical approach

Proactive – not just “looking for bugs”

Infrastructure protection

Cloud infrastructure includes hardware, software, networks, administrative and operations staff, policies and procedures, and the physical data centers that house it all

24 hour monitored
PHYSICAL SECURITY

Centralized
MONITORING AND ALERTS

Update
MANAGEMENT

Anti-Virus/Anti-Malware
PROTECTION

Red Teaming
PENETRATION TESTING

FIREWALLS

Trustworthy foundation

Privacy by Design

Microsoft privacy principles are designed to facilitate the responsible use of customer data, be transparent about practices, and offer meaningful privacy choices.

Microsoft Privacy Standard

Guidelines that help ensure privacy is applied in the development and deployment of products and services.

Data segregation

We use logical isolation to segregate each customer's data from that of others.

Customer Data

When a customer utilizes our cloud services, they retain exclusive ownership of their data.

Control over data location

Customers choose data location and replication options.

Role based access control

Tools support authorization based on a user's role, simplifying access control across defined groups of users.

Encryption key management

Customers have the flexibility to generate and manage their own encryption keys.

Control over data destruction

Deletion of data on customer request and on contract termination.

Data protection

We provide customers with strong data protections – both by default and as customer options

Data isolation

Logical isolation segregates each customer's data from that of others is enabled by default.

At-rest data protection

Customers can implement a range of encryption options for virtual machines and storage.

In-transit data protection

Industry-standard protocols encrypt data in transit to/from outside components, as well as data in transit internally by default.

Encryption

Data encryption in storage or in transit can be deployed by the customer to align with best practices for ensuring confidentiality and integrity of data.

Data redundancy

Customers have multiple options for replicating data, including number of copies and number and location of replication data centers.

Data destruction

Strict standards for overwriting storage resources before reuse and the physical destruction of decommissioned hardware are by default.

Restricted data access

- Customer data is only accessed when necessary to support customer's use of the services (e.g. troubleshooting or feature improvement), or when required by law.
- When granted, access is controlled and logged. (Lock Box)
- Strong authentication, including MFA, helps limit access to authorized personnel only.
- Access is revoked as soon as it's no longer needed.

Access controls are verified by independent audit and certifications.

Law enforcement requests

Microsoft does not disclose Customer Data to law enforcement unless as directed by customer or required by law, and will notify customers when compelled to disclose, unless prohibited by law.

The Law Enforcement Request Report discloses details of requests every 6 months.

Microsoft doesn't provide any government with direct or unfettered access to Customer Data.

Microsoft only releases specific data mandated by the relevant legal demand.

If a government wants customer data it needs to follow the applicable legal process.

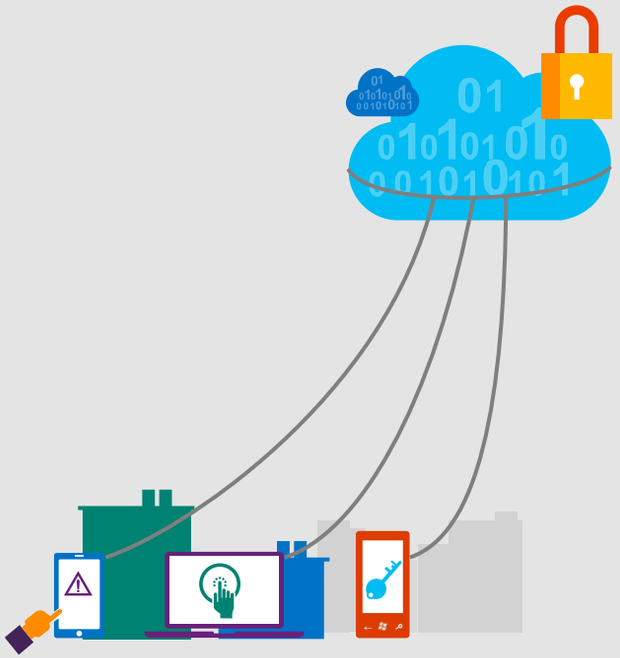
Microsoft only responds to requests for specific accounts and identifiers.

ISO/IEC 27018

Microsoft is the first major cloud provider to adopt the first international code of practice for governing the processing of personal information by cloud service providers.

Prohibits use of customer data for advertising and marketing purposes without customer's express consent.

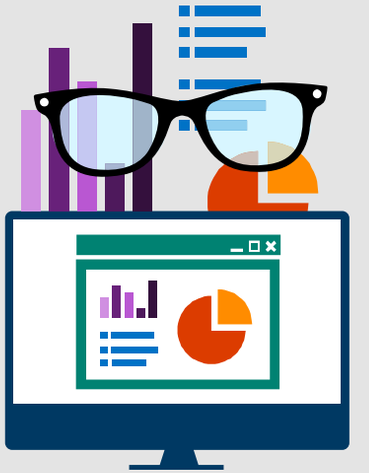
Prevents use of customer data for purposes unrelated to providing the cloud service.



Contractual commitments

Microsoft was the first major cloud service provider to…

- Adopt ISO/IEC 27018 code of practice
- Offer customers E.U. Standard Contractual Clauses that provide specific contractual guarantees around transfers of personal data for in-scope services.
- Have European data privacy authorities validate that its enterprise agreement meets EU requirements on international data transfers
- Abide by US-EU Safe Harbor Framework and the US-Swiss Safe Harbor Program.



Contracting for Cloud Services

1. Service Provider Reputation and Competence
2. Review, Monitoring and Control
3. Audit / Inspection Rights
4. Confidentiality and Certified Security Standards
5. Resilience and Business Continuity
6. Data Location and Transparency
7. Limits on Data Use (No secondary use)
8. Data Segregation / Isolation
9. Conditions on Subcontracting
10. Conditions on Termination


Microsoft