Making privacy accessible to users

GSMA Data Protection & Privacy Conference
29 August 2013, Kuala Lumpur

Valerie Tan
Director Internet Policy
Legal & Corporate Affairs

Microsoft

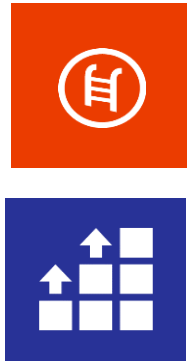
What I will cover

Evolution of Personal Data

Personal Data is increasingly contextual

Evolving Privacy Landscape

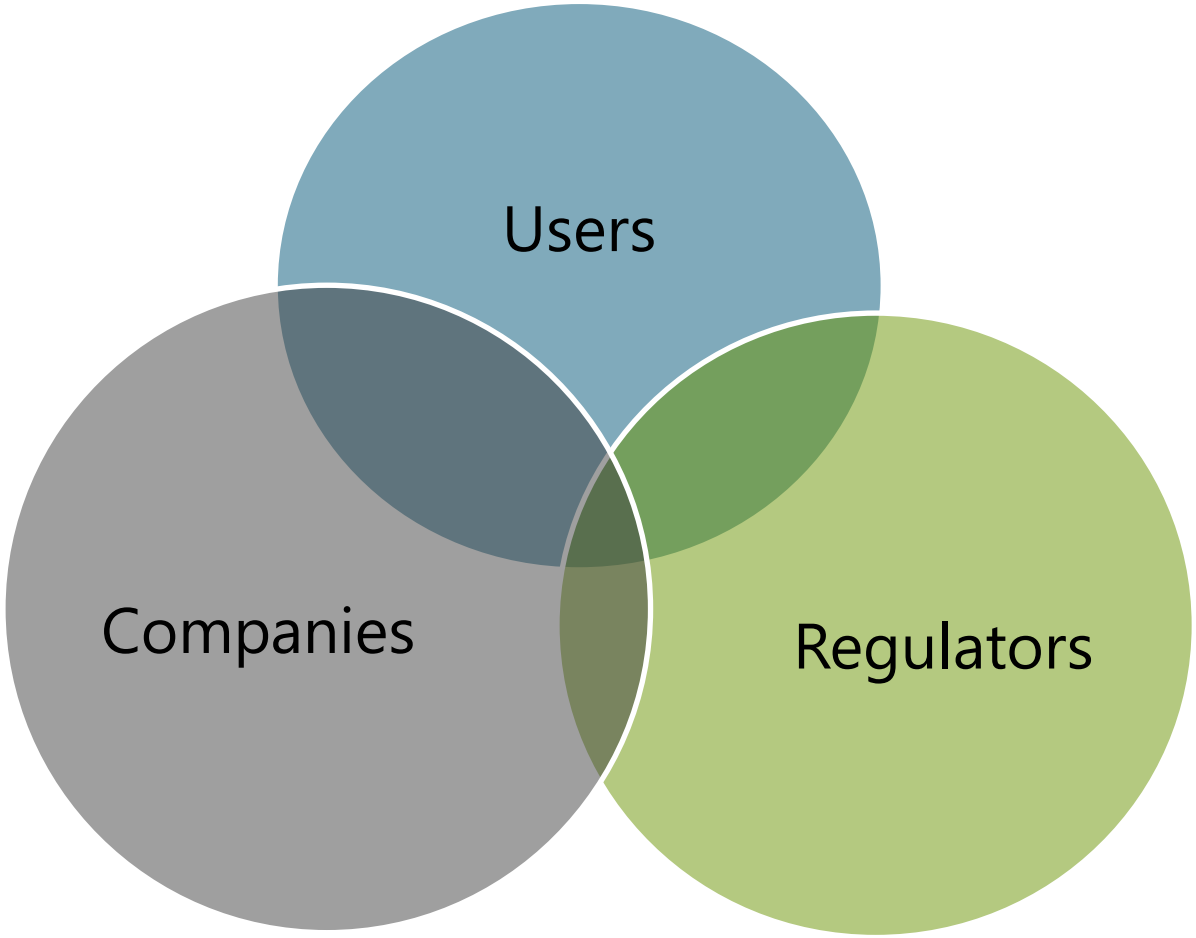
Shifting to a user centric data ecosystem



Flexible Data Governance Framework

World Economic Forum Global Dialogue

Technology and Policy Should Evolve Together



Technology both requires and enables new policy approaches

Sustainable policy framework must balance evolving needs of stakeholders

Findings on User Attitudes Regarding Personal Data

Data context	Seven key variables define a nuanced view of *personal*: **Type of Data** · **Type of Entity** · **Device Context** · **Collection Method** · **Usage/ Application** · **Trust** · **Value Exchange**
Trust and accountability	• Trust is a variable in the data context, but is neither sufficient nor always necessary • Users feel accountable for their decisions. Industry accountability and redress are needed to build trust
Principles-based ecosystem	Users' trust in the ecosystem is enhanced if principles are part of the governance of the data ecosystem
Government's role	Users express concern about government holding their data but preference for government involvement in providing redress and enforcement of industry compliance

Methodology: Qualitative research done jointly with Windows in US, Canada, Germany, China; follow up quantitative research is being planned. Research report published by International Institute of Communications, "Personal Data Management: the User's Perspective," Nov 2012 (http://iicom.org/resources/open-access-resources/cat_view/8-iic-resources/3-open-access-resources/29-personal-data-management)

The Privacy Landscape is Evolving

Past	Today / Tomorrow
User actively participates in transactions where data is collected	Increasingly, data is passively obtained. User not aware of many data transactions.
What is considered personal data is pre-determined	Notion of *personal* is dependent on context of use & subject to (changing) cultural & social norms.
Data is collected for specified use	Discovery / innovation generate economic and social value from commingled diverse data sets.
User consent is required, but user are not empowered	Decentralized data ecosystem makes user consent impractical..
Policy focuses on minimizing all personal risks	Overly conservative approach limits collective social and economic benefits.

Towards a More Flexible Data Governance Framework

There is no bad data, only bad uses of data	Move discussion from data collection to point(s) of use
	Acceptable use is contextual and subject to change
An interoperable metadata-based architecture is required	Metadata reflecting permissions and policy provides the foundation for trustworthy data sharing
Principles should be a core part of ecosystem governance	Provide guidance for trustworthy data practices (preferable to rigid regulation)
	Existing OECD principles nadequate
Codes of conduct supplement principles	Allow for flexibility and differentiation in implementation of the principles
Evidence base informs policy and corporate stakeholders	Economic and social value of data
	Users' attitudes and behaviors regarding personal data

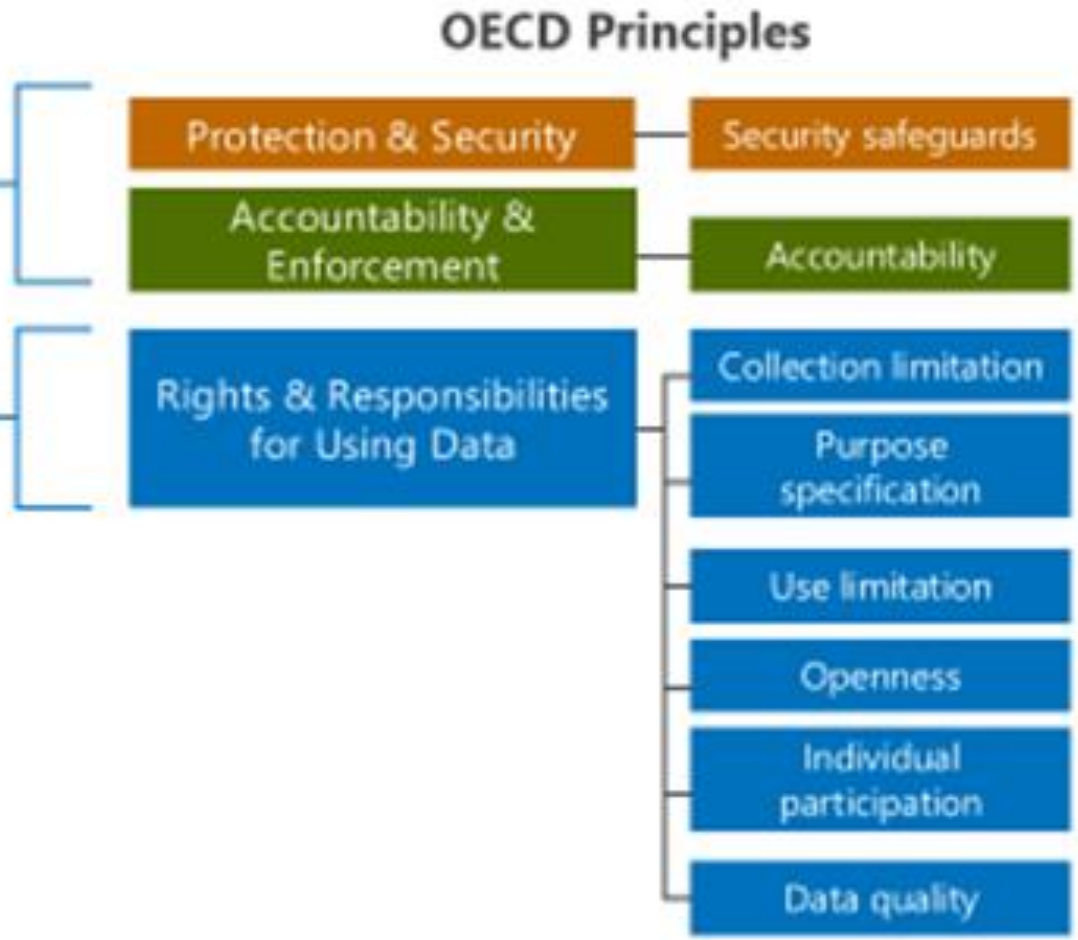
Principles Guiding Trustworthy Data Practices

Some OECD principles are still applicable

Others need to be changed or scrapped

New imperatives for consideration

- User friendly: simplicity & transparency
- User control and changing norms
- Data usage context & onward transfer
- Shared & interoperable permissions
- Change: innovative uses and changing norms
- Fair value exchange



Data Management Principles

Principle	Details
Trust	When users interact with our consumer products and services, they know they are working with Microsoft and that they can **trust us to handle their data in a manner consistent with our data management principles**, regardless of the product or service they are using. We ensure that our products and services comply with our principles and we hold ourselves accountable in this regard.
Transparency	We are open and transparent with users. **We tell them what data we collect from them, what we use the data for, how long we retain that data, and how they can control the use of their data**. We make it clear to users when regulatory compliance or other issues have the potential to change the way we treat their data, and we disclose to the public the number of data requests we receive from government and law enforcement officials.
Innovation and Value	We **use data provided by our users to deliver valuable products and services**. We derive business intelligence and other metadata from user interactions with our services. We use that metadata to improve and protect our products and services, and to protect our users from harm. Within Microsoft, we trust ourselves to innovate with user data in order to deliver new scenarios that are of high value to our users. **We may share data internally amongst product teams, but we expect our Microsoft partners to obtain user consent in cases where new scenarios have the potential to surprise users.** With the user's consent, we make their data available to 3rd party developers so they can deliver innovative apps and services.

Data Management Principles (continued)

Principle	Details
Security and Privacy	We partner with users to keep their accounts and data secure. We expect users to provide complete, verifiable proofs so we can secure their accounts. We request identity data when needed. **We handle sensitive data in a secure manner, encrypting customer communications and obfuscating PII**.
User Control	We differentiate ourselves from the competition through our continued commitment to user data ownership and control. **We design our products and services so users can view, edit and delete their data, and we give them control over how their data is used.**
Retention and Compliance	We retain user data for *active* users forever unless they specifically instruct us to do otherwise. When users delete their data, we honor the delete request[1], but **retain a backup copy of the data on our servers for a period of 60 days to guard against accidental data loss**. We keep abandoned accounts around indefinitely, but we reserve the right to reclaim the *file storage space* for services where storage cost is significant[2]. We comply with existing laws and with legal demands for user data while working to influence regulations we find ineffective or which interfere with our ability to innovate and deliver user value.

[1] We delete user provided data, but not metadata. We perform a “soft delete”, after which data fragments may remain on disk , but it is not accessible without Admin tools. User data will not be removed from log files, backups or data records retained for legal, regulatory or compliance reasons.
[2] Minimum holding period is 2 years