Building Consumer Trust in Electronic Commerce – Panel Response

Interpreting Privacy Principles Symposium
UNSW

Julie Inman Grant
Regional Director, Internet Safety, Privacy and Security
Microsoft Asia Pacific
Changing Privacy Threat Landscape: Diminution of Consumer Trust

- Personal information ultimate “criminal prize” and currency on the web
- Numerous high-profile data breaches reflect inadequate data governance in organizations
- Consumers may not be aware of the tracks they leave when they navigate the web and/or use search services
- Search services raise a number of complex and important privacy issues, and are increasingly a focus of privacy scrutiny.
- Online advertising - big market with new players not familiar with data protection schema
- The emergence of “cloud computing,” and potential privacy risks for health or other sensitive data
- Growth of user-generated content

These trends are driving the policy debates (and the confusion)
Microsoft's Commitment to TwC

Trustworthy Computing

Security
- Secure against attacks
- Protects confidentiality, integrity & availability of data & systems
- Manageable

Privacy
- Protects from unwanted communication
- Controls for informational privacy
- Products, online services adhere to fair information principles

Reliability
- Dependable, Available
- Predictable, consistent responsive service
- Maintainable
- Resilient, works despite changes
- Recoverable, easily restored
- Proven, ready

Business Practices
- Commitment to customer-centric Interoperability
- Recognized industry leader, world-class partner
- Open, transparent

Launched in January 2002
- A Microsoft company-wide mandate
- Intrinsic to Common Engineering Criteria & product lifecycles
- Key consideration when designing product features
End to End Trust Evolution

- Economic Forces
- Social Requirements
- Core Security Components
  - "I+4A"
  - Trusted Hardware
  - Trusted Software
  - Trusted People
  - Trusted Data
- Integrated Protection
  - SDL and SD3
  - Defense In Depth
  - Threat Mitigation
- Secure Foundation
- Political/Legislative
Establishing End to End Trust

**Trusted Stack**
- Needed for a trusted stack
  - HW, SW, people & data validation
  - Robust trust model
  - Informed decisions based on integrity & reputation
- Scalable across all user scenarios

**Core Security Components**
- Identity Claims
- Authentication
- Authorization Policies
- Access Control Mechanisms
- Audit

**Trust Founded on “Identity Claims” not Identity**
- Authenticate users on certified attributes
- In-person proofing
- Protects identity, reveals only data required to be
  - Authenticated
  - Authorized for Access
- Actions auditable, privacy protected
- Stolen identity claim insufficient to cause data breach or ID loss

**Alignment of Social, Political & Economic Forces**
- PII control is right of the individual
- Web anonymity optional but state clear to all parties
- Successful end-to-end trust needs IT solutions aligned with
  - Society
  - Economy
  - Politics/Legislation

People
Software
Hardware
Data
A Growing Patchwork of Laws

A growing jumble of overlapping national, regional and local laws - a daunting and increasingly expensive challenge for organisations

A “global” approach is needed - key principles for global privacy approach:

- A baseline standard applicable across all organisations and industries
  - Strong federal preemption
  - Apply to both online and offline
  - Support international harmonization and cross-border data flows
- Increase transparency through:
  - Privacy notices (including layered notices)
  - Standards for material changes to privacy notices
  - Reasonable access by individuals to personal information about them (with certain important exceptions)
  - Limited and thoughtful breach notification guidelines
- Provide meaningful control over the use and disclosure of personal data
  - Tiered approach to consent based on risk (use vs. disclosure, sensitivity of the personal information)
- Ensure at least a minimum level of security
  - Flexible and scalable
local ref to privacy regulation?

jules, 13/08/2008
ALRC Review: Contribution to Building Trust

- Re-ignited broader public interest in and awareness of privacy
- Principles-based, technology neutral, forward-looking
- “UPPIng” the ante – reducing current fragmentation and inconsistencies in current law
- Reform of health privacy laws should give rise to substantial benefits
- Balanced approach to breach notification (potential tweaks around threshold and liability questions)
- Substantial work will be required in terms of translating concepts into desired policy outcomes but...the debate has begun....
Working Together to Build Trust

- Privacy is critical to the ongoing advancement of the digital lifestyle and social and economic opportunity
- Organisations should consider a multi-pronged approach
- Microsoft is committed to offering leadership in:
  - Technology solutions
  - Progressive and robust internal policies
  - Industry partnerships
  - Customer guidance and education
  - Support for strong legislation and enforcement
- We’re all in this together