Policy recommendations

Personal privacy

The opportunity

Because of the increasing digitization of our lives, vastly more personal data is being generated and collected than ever before. This data can be used to make cloud services more useful, to build better products, and to enable governments, businesses, and researchers to gain new insights into human behavior.

Data is also enabling everyday objects that are connected through the cloud to interact with each other and perform actions that improve lives, drive business efficiency, and power new public services.

Data analytics, machine learning, and artificial intelligence made possible by cloud computing are helping organizations in manufacturing, education, healthcare, and many other sectors understand complex systems, improve efficiency, reduce costs, solve difficult problems, and deliver new capabilities.

The challenge

When businesses and governments hold data that people generate in the ordinary course of daily life using mobile and smartphones and other devices, it understandably creates concerns about the loss of personal privacy, raises fears about the loss of control over decisions made based on algorithms, and increases the risk that observations and predictions based on data analytics will create negative economic outcomes for individuals. People will be reluctant to adopt cloud services if they do not have confidence that their data will be private and secure.

Governments can establish broadly applicable binding legal norms to provide people with legal assurances giving

them confidence that their data is safe in the cloud and that businesses and governments are accountable for the fair use of advanced analytics and algorithmic decision-making.

Policy recommendations

Governments should establish clear, enforceable privacy frameworks that include strong privacy protections while enabling citizens to take advantage of the benefits of cloud computing that are dependent upon data. Privacy frameworks should provide meaningful autonomy for individuals and require organizational accountability for strong privacy protections and fair data use.

Privacy frameworks for the cloud should build on long-standing privacy principles. Chief among these is that people should have reasonable choice over whether personal data is collected and how it is used. To enable informed decision-making, organizations must provide clear explanations about how they collect, store, use, and share personal data.

These and other key principles should be reflected in laws so it is clear to technology companies how they can achieve compliance, but without government mandates for the approaches that companies should take to achieve compliance, as these may become outdated, inhibit innovation, or be counter-productive.

Governments may want to consider the following goals in crafting privacy frameworks for the cloud era:

Promote transparency and control. People should have meaningful control over the use and disclosure of their personal data. To achieve this, privacy information should be provided at

key points in the user experience and people should have access to tools that make it easy to control how their data is collected and used. Where complex data analytics and sensitive data make simple transparency and user control impossible, consumers should expect higher levels of accountability from industry to help ensure the fair use of data, including plain language explanations of analytic processes and steps for remediation of unfair outcomes.

Tailor consent requirements to user expectations. Because data is now collected and used in so many different ways, people can be overwhelmed if constantly presented with privacy choices and requests to consent to data collection. Requiring express consent in every situation could also make it difficult to understand which situations raise serious privacy implications and which are trivial. Consent requirements should be tailored to require express consent in circumstances where people may not expect that data is being collected or where the data being collected is sensitive and personal. Less rigorous consent requirements may be sufficient when less sensitive data is involved or where it will be obvious to people that use of a service entails data collection (for example, when an online shopping service requires a customer's home address in order to deliver purchased goods).

Require organizations to establish sound privacy practices. Privacy laws should require organizations to demonstrate that they have established sound privacy policies that, at a minimum, ensure compliance with legal requirements. This principle should apply to organizations that determine the purposes and means of processing data and those that process data only on behalf of other organizations. It should also apply regardless of where an organization transfers data or whether it engages other organizations to process the data.

Enable data analytics. Privacy frameworks should not be so restrictive that they prevent governments, business, and other organizations from using data analytics to draw insights in an ethical manner. One way privacy frameworks can achieve this while mitigating privacy risks is to encourage the de-identification of data sets so that researchers cannot connect personal data to specific individuals. Where sensitive data and advanced analytics are involved, privacy frameworks should provide businesses and governments with sufficient flexibility to describe the purpose of data collection and the inner workings of analytics techniques in order to enable a broad range of insights and increase benefits to consumers.

Evidence and further reading:

World Economic Forum Report: "Rethinking Personal Data: Trust and Context in User-Centered Data Ecosystems"

IPAA Blog: Ten Steps to a Quality Privacy Program, Part Three: Privacy By Design Tools

Microsoft Blog: EU-U.S. Privacy Shield: Progress for privacy rights

For links to these and other resources, please visit:
http://www.microsoft.com/cloudforgood