



March 29, 2010

Consumer Protection

Privacy Protections Must Reflect the New Realities of Data Collection and Use

by Paula J. Bruening

The recent series of roundtables hosted by the Federal Trade Commission, entitled “Exploring Privacy,” describe an emerging data environment vastly different from the early days of computing. Complex business models, rapidly evolving technologies for data collection, processing and storage, social networking and the flow of data across borders and into the cloud create a world of ubiquitous and pervasive data use. The roundtable discussions revealed again and again that traditional approaches to protecting data are not working: that individuals can only exercise meaningful choice about use of their data in increasingly rare circumstances; that complex technologies and networked business relationships are nearly impossible to describe clearly to the consumer; and that notices in their current form are almost inherently unable to support to make well-considered consumer choices about the use of their data.

Yet when faced with the need to adapt data protection to meet these challenges, the impulse on the part of policymakers traditionally has been to revert to what is familiar—a system of notice and choice—and to attempt fix it, in spite of the fact that notice and choice have proven to no longer serve as a useful starting point when considering effective protection.

As the FTC considers a way toward better protection for consumer data, it would do well to begin not with notice and choice, but by asking how to effectively apply principles of fair information practices in a data environment scarcely imaginable when they were first articulated.

Use-and-Obligations Model

A use-and-obligations model may offer some answers.

A use-and-obligations model suggests that, given the demonstrated limits of choice, use may better serve to trigger an organization’s requirements to protect data. The use of the data, rather than consumer choice, obligates an organization to assume certain responsibilities about the way data is managed and protected. A use-and-obligations model relies upon an organization’s assessment and mitigation of risks raised by data use as a basis for decisions about how it is managed and protected. It takes into account not simply notice and choice, but relies on a fuller complement of fair information practice principles to support the risk analysis—data retention, data quality and integrity, collection limitation, access and correction, use minimization, and security. In a use-and-obligations model, choice would still in some circumstances dictate data

governance, but only in cases where the choice is real. A company's use of data for marketing would depend upon the individual's choice, for example, but its use of data to complete delivery of a good or service would not. Brief, clear notices that provide essential information made available at the time and place meaningful choice is possible would support a use-and-obligations approach. Comprehensive notice would continue to facilitate transparency for regulators and markets.

Principle of Accountability

Such an approach can only work well when coupled with the principle of accountability. Accountability is a well-established principle of fair information practices, but one that has remained largely unexamined by policymakers. Current work on accountability characterizes accountable organizations as responsible and answerable for its data practices and protection. An accountable organization demonstrates commitment to accountability, implements data privacy policies linked to recognized external criteria, and puts in place mechanisms to ensure responsible decision-making about the management and protection of data. An accountable organization must be able to demonstrate that it takes the necessary measures to ensure sound privacy protection, and that those measures yield good privacy results. An accountability approach provides organizations with the flexibility necessary to optimize the value derived from data but imposes greater responsibility on the organization to fairly assess and mitigate the risks those uses pose to individuals. Accountability relieves the individual of the burden of making decisions about data use when those choices will be of little effect, and of policing a complex marketplace against bad actors.

Internationally and domestically, governments, regulators and companies have recognized the need for, and begun to craft new guidance. The Asia-Pacific Economic Cooperative's work on its Privacy Framework and pathfinder implementation projects offers both high level models and possible answers to practical questions and implementation challenges that new approaches may raise. The Centre for Information Policy Leadership guides an effort to develop and accountability framework and the practical tools necessary to make accountability work. The Madrid Resolution proposed international data protection standards. In the United States, The Business Forum for Consumer Privacy continues to refine its work on a use-and-obligations approach. The Future of Privacy Forum and industry associations continue to explore ways to make notice more useful. The FTC should take advantage of the work of these initiatives to advance innovative privacy protections that serve the needs of consumers in the 21st century.

Paula J. Bruening is the Deputy Executive Director of The Centre for Information Policy Leadership at Hunton & Williams LLP.