The Evolution of Information Governance at Intel

Paul P. Tallon, Loyola University (U.S.)
James E. Short, University of California, San Diego (U.S.)
Malcolm W. Harkins, Intel Corporation (U.S.)

Executive Summary
How to govern access to and use of big data is now a critical concern for CIOs as they face a rapidly expanding flood of new data from sources such as RFID, web transactions and social media. Three factors underlie the rise of big data: 1) Access to better, faster and cheaper storage has made it easier for organizations to capture and retain larger amounts of data for longer; 2) Hype about data analytics and the possibility of uncovering important insights through data mining has led to data being retained for long periods even if its analytical value is negligible in the short term; 3) Regulations specify that data has to be retained for specified periods even if it has ceased to be useful for decision-making purposes. These three factors point to two potentially conflicting needs: the need to protect data against various technical and organizational risks and the need to enable greater use of data as a means of generating value.

The full article describes how Intel addressed these conflicting needs through its information governance policy, which initially focused on protecting data but has evolved to a Protect-to-Enable approach that permits potentially risky but value-creating uses of data that were once discouraged.

The Protect Era (2003-2009)
Like many organizations, Intel's initial approach to information governance was to implement policies and structures to lock down access to data. This approach arose from fears that critical systems and data (microprocessor designs and financial data) would be compromised if information governance policies were too lax.

Two events led to the beginning of Intel's Protect Era of information governance. The first was the introduction of Sarbanes Oxley legislation in 2002, which compelled companies to focus more on protecting financial transaction-level data. The second, and more important, was that in early 2003 Intel was impacted by the SQL Slammer virus, which infected its internal networks through an employee's home-based remote network connection. In response, Intel appointed a corporate officer to form a cross-functional Safety and Security task force drawn from every major business unit and significant horizontal functions. This task force focused attention on the need to establish business continuity, risk and security efforts to guard against future attacks on Intel's data.

During the Protect Era, Intel was concerned with mitigating four types of risk: e-discovery, business continuity, compliance and intellectual property. In addition, it contained the risk that IT contractors might pose by introducing non-Intel devices onto its internal network by providing contractors with a fully loaded Intel laptop. The "scorched earth" approach to information governance during this era prevented all unnecessary access to critical information assets. The desire to lock down and protect data resources also led to policies that often mandated retaining data on the most expensive storage devices, in some cases indefinitely. Users were oblivious to the cost of protecting data, and as the volume of data grew data management costs began to escalate.
However, to complete certain tasks, engineers and other workers increasingly applied risky and often unauthorized workarounds that were within the letter, though not the spirit, of Intel’s Protect Era information governance policies. These workarounds increased the level of technical, organizational, reputational and financial risk, offsetting Intel’s attempts to reduce risk. They also prompted a discussion among senior IT leaders on whether an all-consuming emphasis on controls and risk avoidance was likely to prove ineffective or to fail outright. Over time, the protectionist approach to information governance came to be seen as excessive, expensive, risk inducing and detrimental to Intel’s long-term innovation efforts.

The Protect-to-Enable Era (2009 Onwards)
By 2009, BYOD (bring your own device) was emerging as an accepted use of personal technology, and data analytics was gaining momentum. As a consequence, the initial protectionist approach to information governance was increasingly frustrating employees. Intel IT realized that its approach to information governance needed to evolve to become less restrictive and more accommodating of users’ desires to use data or other information resources in new and nontraditional ways. This led Intel to adopt a Protect-to-Enable philosophy toward data management.

Devised by Malcolm Harkins, Intel’s Chief Information Security and Privacy Officer, Protect-to-Enable was intended to generate business value through greater use of IT resources and data but within defined, quantifiable and tolerable risk limits.

Because innovation had long been a driving force behind Intel’s success, management started to view the success of information governance in terms of whether it boosted innovation and reduced time to market. Harkins recognized that the protectionist approach to information governance had held back innovation and increased timescales. For example, Protect-to-Enable facilitated the work of Intel’s business intelligence (BI) data management group, which was formed in 2010. Users wanted self-service BI and analytics capabilities, which often required access to data in other parts of the company. During the Protect Era, data access had been restricted to within a functional area. Analytics challenged that restriction by highlighting the potential for data access to add value in new ways.

Lessons Learned
Eliminate Practices that Over-Govern Information. Management at Intel initially believed that protecting data would minimize risk and drive success. When it became apparent that over-governance was instead driving up costs and increasing risk, the company adopted the Protect-to-Enable approach, which attempts to balance the need to protect data with the need to make it more accessible and available for decision making.

Educate Users about Data-Related Risk and Cost. Intel educated users about the need for information governance by emphasizing the need to: take personal responsibility; be proactive; and work with and not around the policies.

Collaborate with the Business to Design Information Governance. The scope of the governance policy requires the IT group to collaborate with representatives from key business units and functions. Governance rules at Intel were co-created with business representatives with an eye to what is acceptable and appropriate for users in each business area.

Allow Exceptions to Global Policies to Meet Local Needs. A one-size-fits-all approach to information governance is unlikely to work since some policies may conflict with national regulations. For example, the E.U. considers IP addresses to be personal information, requiring additional layers of data protection or precluding the use and storage of this data.

Help Users Put a Financial Value on Data. Intel users assigned a value to their data by working through a data-classification exercise. The value was then used to assess the financial risk of losing the data and to identify the steps needed to reduce the risk to more tolerable levels. It was also used to ensure the data was located on the storage tier whose costs and service levels matched business requirements.

If organizations over-govern their data through bureaucratic and complex structures, or adopt policies that might be perceived by users as restrictive, costly, and time-consuming, there is a risk that users will implement workarounds that completely bypass the governance structure. Rather than using information governance policies or structures to lock down data by controlling its use and access, Intel’s use of Protect-to-Enable has provided an evolving governance framework within which data is effectively shared and used within known and acceptable risk levels.