The Evolution of Information Governance at Intel

This article describes the decade-long evolution of information governance at Intel against a background of rapid increases in data volumes. Intel's initial governance model sought to contain risk by restricting access to key information resources. The model evolved to a Protect-to-Enable approach that balanced the need to protect data with the need to make data more accessible and available for decision making. The information governance lessons learned from Intel's experience can be applied by other organizations.1,2

Paul P. Tallon
Loyola University (U.S.)

James E. Short
University of California, San Diego (U.S.)

Malcolm W. Harkins
Intel Corporation (U.S.)

Big Data and the Need for Information Governance

In recent years, the volumes of data captured and retained by organizations have grown exponentially. In some industries, principally pharmaceuticals, healthcare and energy, the volume of retained data is doubling each year. The huge volume and variety of data now being stored is known as big data. 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. First, access to better, faster and cheaper storage has made it easier for organizations to capture and retain larger amounts of data for longer periods of time. This level of price-performance improvement has increasingly led users to believe that storage is free, so they are not motivated to delete unimportant data. Second, firms are seduced by the hype surrounding data analytics and the possibility of uncovering important insights through data mining. This has led users to retain data for long periods even if its analytical value is negligible in the short term. Third, regulations often specify that data be retained for specified periods even if the data has ceased to be useful for decision-making.
purposes. In some instances, case law has prompted organizations to retain all electronic records indefinitely.\(^4\) 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.

This 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-and-Enable approach that permits potentially risky but value-creating uses of data that were once discouraged. (The Appendix contains more information about the research conducted for this article.) As we argue in this article, the evolution of Protect-to-Enable at Intel reveals a level of maturity that allowed it to avoid a tendency—common across many IT units—to assert control by locking down access to data without a clear and compelling user justification. Protect-to-Enable balances the need to protect data and the need to make data available for exploratory or nontraditional uses. A key aspect of the approach is educating users and working with them to create structures and policies that set boundaries for what is allowed.

We have distilled Intel’s experiences with information governance into five guidelines that can be applied by other organizations. A key lesson is to set information governance policies and structures that enable uses of data within a risk-aware environment.

**Intel Corporation: An Overview**

Although Intel has long been synonymous with microprocessor innovation, the company sees itself as more than a microprocessor company. Since the early/mid 2000s, Intel’s strategy has evolved from a focus on designing and manufacturing microprocessors to delivering IT-based solutions that encompass aspects of microprocessor design but that can equally include software platforms and services. The bulk of Intel’s revenues and profits continue to come from two of its five business units: PC Client Group (64% of sales; 89% of operating income) and Data Center Group (20% of sales; 35% of operating income).\(^5\) Both groups encompass Intel’s traditional microprocessor products that are used in desktop PCs, laptops and servers.

Like many organizations, Intel has struggled to manage its vast pool of data. By mid-2013, it was managing over 65 petabytes of data—150 times larger than the digital archives of the U.S. Library of Congress. This staggering volume of data has grown at 30% to 40% per annum for most of the last decade, easily swamping any percentage increases in sales and profitability. More importantly, the growth in data volume has occurred at a time when IT spending has declined from 3.5% of sales in 2004 to 2.4% in 2011. A particularly vexing aspect of this growth involves unstructured data,\(^6\) which has grown faster than structured data and is more difficult to govern. Approximately 58% of Intel’s data is unstructured engineering files that are used in product design. The complexity and scale of these files have increased with each new generation of microprocessor.

Intel’s data challenges are further compounded by the global nature of its operations with seven fab plants in four countries (China, Ireland, Israel and the U.S.) and seven assembly, test and R&D facilities in five countries (Costa Rica, China, Malaysia, the U.S. and

---

\(^4\) Case law based on previous judgments comes from two main sources. The first involved a $1.57 billion judgment in 2005 against Morgan Stanley in favor of investor Ron Perelman arising out of his acquisition of Sunbeam. The court had requested specific data from the defendants only to be told, falsely, that no such data existed. The judge imposed punitive damages of $1.45 billion because of the defendant’s failure to comply; the entire judgment was later reversed on appeal. In the second case, involving Zubulake v. UBS Warburg (2004)—a case alleging gender discrimination, failure to promote and retaliation—the judge criticized the defendant for insufficient e-discovery and destruction of documents. This case established the requirement for firms to produce data in court in a timely manner. Corporate legal counsel has reacted to these decisions by requesting that all data be retained indefinitely.


\(^6\) Unstructured data refers to standalone files that exist separate from the applications that created them. Examples include digital media files (voice or video), CAD, office files (word processing or spreadsheets), email, web files and text documents. Because it is unstructured, such data is difficult to govern. For example, depending on the content, sender or recipient, some emails may need to be retained for significant periods of time. Metadata (data about data) is often used to describe unstructured data. In the case of email, this could be a subject line, although subject lines rarely describe with sufficient detail and accuracy the complete contents of each email.
Vietnam). Each of these seven countries operates a different set of directives and recommendations pertaining to privacy policies, data security, ownership, retention and use.

The Protect Era of Information Governance (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, such as microprocessor designs and financial data, would be compromised if information governance policies were too lax.

The origins of information governance at Intel can be traced back to 1992 with efforts to consolidate and centralize network and mainframe IT, which had been distributed and locally managed by individual business units and sites. Table 1 provides a general timeline of the company’s information governance initiatives from 1992 onwards. Desktop computing was centralized in 1995, although applications remained under local control until 1998 when a second IT unit (the e-business group) was created to bring applications under central control. This dual approach to IT management—one IT function managing all aspects of IT hardware with a separate IT function managing applications—remained in effect until 2004 when a single IT function with one CIO and a consolidated IT budget was formed to control all aspects of IT across all of Intel’s business units and locations worldwide.

As part of the IT consolidation in 2004, Intel’s Information Management (IIM) group initiated a Master Data Management (MDM) program. To support this effort, Intel was anxious to create a single set of MDM policies. IIM needed a governance process that would engage business people across the enterprise in setting these policies. Intel also needed policies that would reflect different regional laws and the changing nature of Intel’s activities. To that end, IIM created independent information governance boards for each of its six core master data areas: customer, supplier, location, item, worker and finance.

Two events led Intel to implement strong protectionist policies over data. First, the introduction of Sarbanes-Oxley legislation in 2002 compelled the company to focus more on protecting financial transaction-level data. Second, and more importantly, in early 2003,

---

7 Intel’s fab plants are considered chemical facilities under the 2011 Chemical Facility Anti-Terrorism Security Act. While the act articulates the need for physical access controls, it also specifies the need to protect key information.

8 Research shows that one of the first steps towards effective information governance is to use a consistent approach to data management across the enterprise. See Khatri, V. and Brown, C.V. “Designing Data Governance,” Communications of the ACM (53:1), January 2010, pp. 148-152; and De Haes, S. and Van Grembergen, W. “An Exploratory Study into IT Governance Implementations and its Impact on Business/IT Alignment,” Information Systems Management (26:2), March 2009, pp. 123-137.
Intel was impacted by the SQL Slammer virus, which infected Intel’s internal networks through an employee’s home-based remote network connection. In response, Intel’s CEO, Andy Grove, placed a corporate officer in charge of forming a cross-functional Safety and Security task force drawn from every major business unit and significant horizontal functions such as finance, HR, IT, environment, health and safety, corporate security and legal. This task force focused attention on the need to establish business continuity, risk and security efforts to guard against future attacks.

This marked the beginning of Intel’s Protect Era of information governance. Efforts to lock down access to Intel’s key IT assets were expanded in 2005 in advance of the consolidation and centralization of manufacturing and factory systems in 2006.

Intel was concerned with four types of risk:

- **e-discovery**: the ability to efficiently search, locate and recover key information within a given time interval, often as a result of a court order
- **Business continuity**: the ability to recover critical business operations with minimal long-term disruption
- **Compliance**: satisfying minimum standards for data retention, controls and access
- **Intellectual property**: cyber-attacks, theft or access violation.

One way Intel managed these risks was by regularly involving legal counsel in setting information governance policies. Legal counsel helped to interpret the ever-growing body of legal requirements and to set retention limits for various types of data, not only for e-discovery but in other cases where Intel IT might not fully grasp the legal ramifications of losing data.

Another manifestation of the Protect Era was Intel’s approach to IT contractors. At the time, Intel adjusted its IT staffing needs through short-term contracting. To contain the risk that IT contractors might pose by introducing non-Intel devices onto Intel’s internal network, it provided contractors with a fully loaded Intel laptop.

The resulting Scorched Earth approach to information governance prevented all unnecessary access to critical information assets. The result, however, was an increase in individuals devising policy workarounds. Management discovered that to complete certain tasks, engineers and other workers applied risky and often unauthorized workarounds that were within the letter, though not the spirit, of Intel’s 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. As Intel’s Chief Information Security and Privacy Officer noted about Intel IT’s tendency to over-protect the company’s data:

> “When we just focused on protecting data, we had an over-control situation. We over-constrained and eventually generated more risk because people could figure out a way to go around the controls.”

Intel’s 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; chargeback models were not formally used to assign costs to specific users. As the volume of data grew, data management costs began to escalate. A member of Intel’s Cloud Integration efforts observed how user behavior contributed to increased IT costs:

> “Information growth and user behaviors are driving up IT infrastructure costs. The only way we can change that is to transition to a requirement-driven organization where if we understand the value of information and how to unlock that value, we can start to align value to data storage infrastructure.”

### The Protect-to-Enable Era of Information Governance (2009 onwards)

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. By 2009, BYOD (bring your own device) was emerging as an accepted use of personal technology, and data analytics was gaining momentum in the practitioner literature. As a consequence, the initial 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\(^{10}\) was intended to generate business value through greater use of IT resources and data but within defined, quantifiable and tolerable risk limits. Harkins explained management’s thinking on why governance policies from the Protect Era needed to be replaced:

“Our whole protectionist stance might have mitigated one form of risk but it increased other forms of risks. I think we would’ve had a lower cost and risk portfolio if we reacted differently. But, because I went Scorched Earth and reacted to what introduced harm to the company, I over controlled instead of appropriately controlling with a more nuanced and sophisticated approach. If we had allowed an unmanaged device on our network and had been more open to that dialog earlier, we would have designed controls earlier around being more progressive on BYOD. I made a risk decision. It was an imperfect decision but we let it stay in place too long and we never looked back. We would’ve been more innovative and we would’ve enabled the company more at a lower cost point if we had changed sooner. But, we didn’t really make the switch to Protect-to-Enable until about 2009.”

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. Cost savings were also a consideration. Therefore, an important element of Protect-to-Enable was communication with and education of users so they would learn how data management costs grow. An Enterprise Storage Architect at Intel observed:

“One of the biggest issues we had [before Protect-to-Enable] involved the lack of a proper cost model where we could charge users based on their use of storage. Users were able to dictate that they just wanted the fastest, the most smoking-hot storage irrespective of the criticality of the data. Under Protect-to-Enable, we now have a process where business needs and data classification [the value of data] are taken into account. A user is now given a cost associated with their storage usage and in a lot of cases you’ll find that when they get the dollar figure, they realize that they don’t need that level of performance or protection and can make do with a lower tier of storage. [However] if the user says they don’t want to spend that amount of money [and] if Intel thinks the data is critical, data stewards will work with management to get that money. They’re not going to allow users to keep critical data on a lower tier, just because users don’t have enough money. The risk would be more than we want to tolerate.”

An important factor in Intel’s transition to Protect-to-Enable was changing how users viewed data management. A member of Intel’s Cloud Integration efforts highlighted an evolving role for data users:

“One issue we’ve seen as we move to an enablement model is the need to convince the various lines of business that they—not Intel IT—are the stewards of the data. They need to take ownership of their data including classifying its value and how it should be used before we can decide the mechanics of how the data will be managed. They know the value of their data better than we [Intel IT] do so we have to rely on them to provide that insight.”

An Enterprise Storage Architect outlined the governance process by which users or data stewards classify data according to its value and

\(^{10}\) For more information, see Harkins, M. Managing Risk and Information Security: Protect to Enable, ApressOpen, 2013.
The Evolution of Information Governance at Intel

how this outcome has implications for how data is managed.\footnote{1}{For further details on how Intel has structured its internal storage environment, see Bell, R. et al. “Solving Intel IT’s Data Storage Growth Challenges,” IT@Intel White Paper, January 2012; and Srinivasan, V., The Evolution of Master Data Management at Intel: A Case Study of Finance Master Data, April 2011 (http://www.dataversity.net/the-evolution-of-master-data-management-at-intel/).}

“We require a review process that’s primarily designed for business continuance. Users go through a questionnaire that finds the criticality of the data based on business needs and whether it is actually critical or just business-important. Based on that outcome, we can place data on an appropriate [storage] tier.”

Responsibility for applying Protect-to-Enable across the enterprise was vested in Intel's Corporate Risk and Security Group (CRSG), whose responsibilities covered all electronic and paper records across all U.S. domestic and international locations, business units and employees. Its primary goals were:

1. Develop and administer guidelines for the retention and disposition of data; promote compliance by Intel employees and outside contractors with the guidelines and, where appropriate, with all international legal/regulatory mandates
2. Maintain corporate records in compliance with all legal obligations and preserve information if Intel is involved in litigation
3. Manage Intel information for which there is no legal or regulatory requirement or business need
4. Protect the privacy of information as required by law, regulation and Intel’s privacy policies.

The CRSG assumed many of the strategic policy-making activities previously assigned to the governance boards that had overseen the MDM initiatives begun in 2004. The focus now was on evolving information governance to include data architects who understood the complexities of capturing and retaining massive amounts of data, and business leads (the ultimate owners of the data) who understood how data could be better applied for decision making. While governance boards were still able to focus on technical MDM issues such as ensuring integration and consistent data standards across all critical applications, policy setting was vested in an Ethics and Compliance Oversight Committee within the Risk and Compliance function of Intel.

Given the strategic focus of this committee, representatives were drawn from critical support groups such as IT, HR, legal, business development and internal audit, with other representatives drawn from key business functions such as sales and marketing, manufacturing and product design. This committee continues to meet on a quarterly basis to review and, where necessary, propose information governance policies for each business unit and country. Business units are expected to conduct self-assessments periodically to determine if their policies are adequate for their needs and consistent with Protect-to-Enable, or if they should be expanded to account for new risks or changes within the business unit operating environment.\footnote{2}{For an analysis of how storage decisions reflect a balance of cost and risk, see Tallon, P. and Scannell, R., op. cit., 2007; Weber, K., Otto, B. and Österle, H. “One Size Does Not Fit All: A Contingency Approach to Data Governance,” Journal of Data and Information Quality (1:1), 2009, pp. 1–27; Tallon P. P. “Understanding the Dynamics of Information Management Costs,” Communications of the ACM (53:5), 2010, pp. 121–125; and Bell, R. et al., op. cit., 2012. For information on how to design data governance structures and policies that balance cost and risk, see Khatri, V. and Brown, C. V., op. cit., 2010.}

The operational aspects of Intel’s information governance are currently managed through technical IS roles and activities within Intel IT. Audits are used to check compliance with information governance rules and to propose high-level policy changes where necessary. Intel IT also conducts risk assessment and incident-response planning activities that tie back to the oversight work of the Ethics and Compliance Committee. Operational activities also include data backups and disaster recovery planning because both activities are critical to maintaining an adequate level of user access to data for decision making.\footnote{3}{The value of backups is assessed by two metrics: RPO (return point objective based, on the age of the last backup) and RTO (return time objective or the length of time needed to restore from backups).} Intel IT also plays a key role in monitoring information governance for compliance with domestic and international regulation. Internal audit and Intel’s Security and Privacy Office monitor the internal and external
landscapes for unfolding threats and other factors that could cause information risk to increase to unacceptable levels.

Intel considers external engagement to be a core element of information governance. Information about threats and vulnerabilities, best practices and benchmarking is widely shared with professional IS groups, such as the Information Risk Executive Council and the San Francisco Bay Area CSO Council. Such engagements help to highlight external factors that could affect information governance at Intel.

How the Protect-to-Enable Approach Facilitates Analytics

Adopting a Protect-to-Enable approach to information governance in 2009 was fortuitous in light of the growing popularity of data analytics that emerged by the end of that decade. In 2010, Intel created a business intelligence (BI) data management group whose goal was to facilitate the collection, processing, retention and distribution of data needed for analytics. The desire among users for self-service BI and analytics capabilities forced Intel to reassess its information governance since data analytics often required access to data in other parts of the company. Part of the task of building analytics capabilities was allowing functional areas to see the value of their data when shared outside their immediate area. During the Protect Era, data stewards had restricted data access to within their functional areas. Analytics challenged that restriction by highlighting the potential for data access to add value in new ways.

Although MDM was no longer a limitation, users had no incentive to share data or even to publish its existence. Hence, some degree of data duplication existed before a firm-wide data analytics effort was established. The BI data management team began to function as a broker between users and owners of the data. Thus, the Protect-to-Enable approach moved information governance beyond the perspective of who owns the data to who can best use the data and what types of organizational value they might achieve from using data in new ways.

Measuring the Value of the Protect-to-Enable Approach

Intel is well known for its intense metrics-driven culture. Because of the strategic role of data in Intel, the company monitors changes in costs (how data growth is impacting IT spending), in risk (how much value is lost if data is lost or compromised) and in value (how data is helping to improve firm performance).

The company evaluates the Protect-to-Enable approach in a similar way. Technical and business risk are consistently monitored through systems audits, while data storage costs are tracked to determine whether resources are being wasted or if spending targets are being met. Value is measured in operational and strategic terms. A decline in data loss and security-related incidents that put data at risk indicates, at an operational level, whether data is being adequately protected. At a more strategic level, Intel uses agility as a measure of its ability to respond to market change and to design, test and deliver new products and services within an ever-shorter timeframe. For example, analytics has helped Intel to cut 25% off the time needed for chip design validation, thereby allowing it to launch products faster than its competitors and so maintain its lead in the microprocessor market. As an innovator, Intel examines whether data is enabling new growth opportunities and how data can benefit productivity and the overall effectiveness of its manufacturing operations.

In this way, Intel monitors both aspects of Protect-to-Enable—whether data is protected and whether data is enabling new opportunities for improving financial performance and market positioning.

Lessons Learned

Five key lessons emerged from Intel's experience. These lessons can be applied by other organizations as they seek to develop information governance—or to benchmark their current


16 Users are often under the mistaken belief that falling hardware costs allow for a greater level of data retention. In reality, however, for every dollar spent on storage hardware, three to seven dollars goes to non-hardware items such as labor and support expenses, software licensing and datacenter support costs.

practices as they respond to the emergence of big data.

1. Eliminate Practices that Over-Govern Information

Management at Intel initially believed that data protection would minimize risk and drive success. There was little tolerance for data-driven risk, and it was relatively easy to implement policies to limit data access. When it became apparent that over-governance was instead driving up costs and increasing risk, management sought to identify and remove practices that were too restrictive. The Protect-to-Enable approach attempts to balance the need to protect data from various risk factors with the need to make data more accessible and available for decision making.

2. Educate Users about Data-Related Risk and Cost

Users may have minimal understanding of the costs associated with managing information. They tend to see information management costs purely in terms of purchase prices and fail to recognize that these costs are a fraction of the total cost of ownership. They also fail to appreciate the different types of risk and how their actions and behaviors can contribute to higher risk.

When organizations develop information governance policies and structures, users may not immediately understand why their actions are being regulated. They are focused on doing their jobs, not on the costs or risks of doing that job. Intel repeatedly educated its users as to why specific policies were in place. The goal throughout was to encourage users to work within the letter and spirit of Intel’s information governance policy framework and then to trust them to act appropriately. Given the sharp rise in data costs, Intel also used a cost-allocation model to report data-specific costs to users (this is not a traditional chargeback model but rather an informational model).

Intel’s approach to educating users about both the need for information governance and sensitivity to risks and costs can be summarized as:

- **Promoting personal responsibility:** since unstructured data accounts for a disproportionate share of storage costs and risk, users should be discouraged from unnecessary data hoarding and retention of files that are clearly of no future value, while encouraging more accurate assessment of storage needs.

- **Being proactive:** users will likely think that the data they use in their job is of the highest value to the organization and, therefore, appropriate for retention on tier 1 (the most expensive) storage. Data is rarely so valuable and, hence, users should be educated to quantify value and, where possible, to move their data to a lower storage tier.

- **Working with and not around policies:** information governance best practices are evolving often in response to system failures or other adverse storage events. Since users may not always see the business logic behind each policy, information governance may be seen more as an obstacle than as an enabler of work. Bottom-up approaches to information governance, where each business unit or function is allowed to develop its own rules, fosters unnecessary complexity and inconsistency. If policy deviations are necessary, they should be decided by a corporate-wide function.

3. Collaborate with the Business to Design Information Governance

While responsibility for information governance may, by default, be assigned to the IT group, the scope of the governance policy requires the IS group to collaborate with representatives from key business units and functions. An important feature of the Protect-to-Enable approach at Intel was its collaborative nature; rules were not imposed on users in a way that might breed resentment. Instead, governance rules were co-created with business representatives with an eye to what is acceptable and appropriate for users in each business area.

4. Allow Exceptions to Global Policies to Meet Local Needs

Multinational corporations with significant operations outside the U.S. face additional
challenges in managing information. A one-size-
fits-all approach 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. Intel had to grapple with bring-your-own-device policies that limit device monitoring in some markets. It regularly assesses global policies and customizes local policies to meet unique regional or market needs.

5. Help Users Put a Financial Value on Data

Intel discovered that it is difficult to put a financial value on data, but users were still expected to work through a data-classification exercise to assign a value to their data. From this value, Intel IT computed the financial risk of losing the data and identified the steps needed to reduce risk to more tolerable levels. Over time, data stewards emerged as important stakeholders in helping to monitor changes in value. As the financial value of data shifted over time, Intel was able to migrate its data to appropriate storage tiers whose costs and service levels matched business requirements.

Concluding Comments

Forecasters predict that by the end of the next decade, the quantity of data under management in many organizations and business sectors will increase fifty-fold. Even the most conservative estimates of 40% annual growth imply a twenty-fold increase in the amount of data by 2020. Like many organizations, Intel recognized the strategic value of its data and the need to carefully manage data in ways that allow value to be realized within tolerable risks limits. 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 provided an evolving governance framework within which data was effectively shared and used within known and acceptable risk levels.

As data analytics becomes an increasingly important driver of sales growth and financial performance, managers will likely rely on information governance to determine what they can and cannot do with data. 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. The risk of operating outside formal governance structures is that users may not readily grasp the risks of losing data. The point is not to avoid information governance entirely or to employ minimally intrusive policies but to educate users and work with them to create structures and policies that set boundaries for what is allowed.

Appendix: Research Methodology

In addition to information provided by Malcolm Harkins (the Intel co-author of this article), the academic co-authors conducted semi-structured interviews with seven subject matter experts at different levels in Intel IT. Interviews were tape recorded and transcribed. We then used content analysis on each transcript to reveal the history of information governance at Intel, the range of information governance practices in place, the risks these practices were intended to address and their overall level of success.

---

18 E.U. members have been given some flexibility in deciding how to apply the 1995 Data Protection Directive, which prescribes the need for information governance. The Article 29 Working Party (the E.U. Committee tasked with clarifying the directive) declared in 2007 and 2008 that IP addresses are personal data since they relate to an “identifiable person.” Adding to the confusion, in 2008, a German court issued a contradictory ruling saying that IP addresses are not personal data and do not need to be protected as such. As of 2013, the E.U. is planning a comprehensive review of the 1995 directive to take account of new innovation and legal/compliance challenges. Outside the E.U., interpretations of the personal nature of IP addresses vary widely.

About the Authors

Paul P. Tallon
Paul Tallon (pptallon@loyola.edu) is Associate Professor, Frank J. DeFrancis Chair in Information Systems and Director of the Lattanze Center for Information Value at the Sellinger School of Business, Loyola University, Maryland. Previously, he was an IT auditor and accountant with PricewaterhouseCoopers. He has published over two dozen papers in journals including MIS Quarterly, Journal of Management Information Systems, European Journal of Information Systems, Journal of Strategic Information Systems and Communications of the ACM. He won the 2007 Journal of Management Information Systems paper of the year. His research interests cover the economic impacts of IT, strategic IT alignment, real options, IT risk and the economics of information management.

James E. Short
James Short (jshort@ucsd.edu) is Lead Scientist, Center for Large-Scale Data Systems, at the San Diego Supercomputer Center, University of California, San Diego. Previously, he was on the faculties of the MIT Sloan School of Management and the London Business School. His work has been published in The Accounting Review, MIS Quarterly, Journal of Management Information Systems, Journal of Management Studies, International Journal of Communications and Sloan Management Review. His research interests cover the value of data and information growth, information transparency and financial performance, and data metrology and measurement.

Malcolm W. Harkins
Malcolm Harkins (malcolm.harkins@intel.com) is Vice President and Chief Information Security and Privacy Officer at Intel Corporation. In this role, he is responsible for managing the risk, controls, privacy, security and other related compliance activities for all of Intel’s information assets, products and services. He was previously Chief Information Security Officer and has held several other roles at Intel spanning finance and procurement. He was recognized by Computerworld magazine as one of the top 100 IT Leaders for 2012. He is the author of several Intel white papers and, most recently in 2013, his first book, Managing Risk and Information Security, Protect to Enable, was published by ApressOpen.