Protecting Privacy in Big Data: A Layered Approach for Curriculum Integration

Dana Schwieger
dschwieger@semo.edu

Christine Ladwig
cladwig@semo.edu

Department of Accounting
Southeast Missouri State University
Cape Girardeau, MO 63701, USA

Abstract

The demand for college graduates with skills in big data analysis is on the rise. Employers in all industry sectors have found significant value in analyzing both separate and combined data streams. However, news reports continue to script headlines drawing attention to data improprieties, privacy breaches and identity theft. While data privacy is addressed in existing information system (IS) programs, greater emphasis on the significance of these privacy issues is required as big data technology advances. In response to this demand, some colleges and universities are developing big data programs and degrees (Gupta, Goul & Dinter, 2015). Yet not every university has the resources to allow for such expansion; some institutions struggle just to cover their IS core program courses. For these latter programs, awareness of the importance of privacy and privacy methods—like the application of security controls—is best integrated academically through a layered approach. Therefore, in this paper, the authors illustrate the important role that data privacy plays in the realm of big data, and suggest methods for providing a layered approach to applying big data privacy concepts to the IS2010 Model Core Curriculum.

Keywords: Big Data, Privacy, Teaching Methods, IS2010 Model Curriculum

1. INTRODUCTION

The ever-increasing capabilities of technology to access, collect, disseminate and manipulate growing stores of data are opening new doors for researchers, industries, businesses and…cybercriminals. Proper application of big data analysis has the potential to improve accuracy, timeliness, and relevance of corporate operations (Landefeld, 2014). However, future employees need to be aware of the critical role of data privacy in every organization's analysis of big data, as well as the consequences that may ensue if efforts are not reasonably made to protect confidentiality. In this article, the authors describe the need for privacy awareness among students in the expanding world of big data and, using the IS2010 Model Curriculum Guidelines, suggest areas in which big data privacy methods can be incorporated into the curriculum to provide a constant reminder of the significant role that privacy plays in organizations' future success or failure.

2. BIG DATA AND PRIVACY: "FIRST, DO NO HARM."

"Information is the oil of the 21st century, and analytics is the combustion engine." - Peter Sondergaard, Senior Vice President, Gartner Research

Background

They all agreed it was a great idea—the creation of an open source software program to "safely organize, pool, and store student [K-12] data from multiple states and multiple sources in the cloud" (Kamenetz, 2014, para. 2). Such a big data system would revolutionize student learning throughout the country, and promote educational progress on many levels. The planned program, organized within the not-for-profit company inBloom, Inc., would include "everything from demographics to attendance to discipline to grades to the detailed, moment-by-moment, data produced by learning analytics programs like Dreambox and Khan Academy" (Kamenetz, 2014, para. 2). The data could be accessed by educators through an application-programming interface (API), essentially making the information universally available to any school, with only minimal inputs. In 2011, the Bill and Melinda Gates Foundation got behind the project, dedicating over $87 million to develop the shared learning infrastructure. It was an educators' dream come true.

inBloom's Downfall

As the company moved forward with the project, it partnered with nine states representing 11 million students: Colorado, Delaware, Georgia, Illinois, Kentucky, Louisiana, Massachusetts, New York and North Carolina (Kamenetz, 2014). But shortly after collaboration began, the shared big data dream began descending into an unexpected privacy nightmare. It was reported by Reuters that the $100 million database held files where "millions of children [were identified] by name, address and sometimes social security number. Learning disabilities [were] documented, test scores recorded, attendance noted. In some cases, the database tracked student hobbies, career goals, attitudes toward school—even homework completion" (Simon, 2013, para. 3). And although local education officials retained control over their respective students' information, federal law would allow them to "share files in their portion of the database with private companies selling educational products and services" (Simon, 2013, para. 4).

Parents in the partnership states were astounded at both the type of data collected and its handling; a firestorm of protests against the system began in Louisiana, Colorado and New York. As a result, inBloom spent the majority of their project development days addressing privacy concerns and attempting to keep their state partners in the program. The company's initial policy statement did little to aid in their battle: "inBloom, Inc. cannot guarantee the security of the information stored in inBloom or that the information will not be intercepted when it is being transmitted" (Madda, 2014, para. 19). Louisiana was the first state to back away from the inBloom database when "State Superintendent John White agreed to pull student data out…in April, 2013. By August 1, 2013, five of inBloom's state partnerships were kaput" (Madda, 2014, para. 21). A few months later, with no remaining partners, the company announced the end of the project (Bogel, 2014).

The rise and fall of inBloom's big data project was directly related to the measure of privacy (or lack thereof) afforded by the database. While most would agree that big data provides for a better understanding of information critical to the success of modern businesses and our broader society, it is also clear that the increasing need for privacy is a forefront concern. With over 40% of mid-market businesses already engaged in one or more big data projects, and another 55% of businesses contemplating a project in the near future, it is important that information technology students become familiar with big data privacy issues (Dell, 2014). Up-and-coming information systems managers would do well to ignore Facebook founder Mark Zuckerberg's sentiment that "Privacy is dead"—at least where big data is involved (Craig & Ludloff, 2011).

Incorporating Privacy into the Curriculum

This paper describes the need for privacy in the expanding world of big data, as well as a review of the methods that are currently available to protect such privacy. Although some universities are addressing the commercial need for Big Data analysis skills by creating new courses and programs, many institutions require a more conservative option. The authors therefore suggest integrating expanded big data privacy concepts into the IS 2010 Model Core Curriculum using a layered approach. This approach allows existing courses to highlight these very important privacy concepts without overwhelming an already substantial curriculum base.

The value of training information technology students in privacy procedures parallels the importance of other critical big data records management techniques. In the May 2014 report "Big Data and Privacy: A Technological Perspective," U.S. Presidential Science and Technology Advisors recommended the expansion of education in the area of big data and privacy, hoping to "accelerate the development and commercialization of technologies that can help to contain adverse impacts on privacy, including research into new technological options.

By using technology more effectively, the Nation can lead internationally in making the most of big data's benefits while limiting the concerns it poses for privacy" (President's Council of Advisors on Science and Technology, 2014, p. 9).

3. BIG DATA AND PRIVACY: WHAT'S THE "BIG" DEAL?

The benefits of big data are proving to be highly valuable; businesses have been able to profile and target consumers, redevelop more marketable products, create new revenue streams, and reduce maintenance costs—all in record time (Dataseries, 2012). But as with any fast-growing technology, there are associated risks. Privacy issues have been identified as a primary risk; and the mismanagement of big data with respect to privacy may also result in loss of compliance and other regulatory problems as well (Tobin, 2013). Privacy scholars have also discussed a second risk closely associated with big data privacy: potential discrimination (Rubenstein, 2012). Michael Schrage, in a Harvard Business Review article, points out "in theory and practice, big data digitally transmutes cultural clichés and stereotypes into empirically verifiable data sets. But the law, ethics and economics leave unclear where value-added personalization and segmentation end, and harmful discrimination begins" (Schrage, 2014, para. 10).

In a report by the Massachusetts Institute of Technology (MIT), Georgetown University Law Professor David Vladeck discusses what some believe is the greatest privacy risk associated with collected big data, that "consumers will suffer 'discrimination by algorithm', or a kind of data determinism, because correlation will lead individuals to be categorized . . . [based on] general trends that will be seen as sufficiently robust to draw conclusions about their individual behavior, often with no process for mitigation if the conclusion is wrong" (MIT Workshop, 2013, p. 8). White House Science and Technology Advisors echoed this concern in their own report, citing "data analytics discovers patterns and correlations in large corpuses of data, using increasingly powerful statistical algorithms. If those data include personal data, the inferences flowing from data analytics may then be mapped back to inferences, both certain and uncertain, about individuals" (PCAST, 2014, p. x).

Even if the data interpretations are valid, the use of such data can lead to personal harm. The Presidential advisors present in their report some actual and potential examples of big data applications and their inferred privacy concerns:

- "The UK firm FeatureSpace offers machine-learning algorithms to the gaming industry that may detect early signs of gambling addiction or other aberrant behavior among online players.
- By tracking cell phones, RetailNext offers bricks-and-mortar retailers the chance to recognize returning customers, just as cookies allow them to be recognized by on-line merchants. Similar WiFi tracking technology could detect how many people are in a closed room (and in some cases their identities).
- The retailer Target inferred that a teenage customer was pregnant and, by mailing her coupons intended to be useful, unintentionally disclosed this fact to her father.
- The author of an anonymous book, magazine article, or web posting is frequently "outed" by informal crowd sourcing, fueled by the natural curiosity of many unrelated individuals" (PCAST, 2014, p. 12).

Numerous factions report that big data privacy concerns are especially prominent in healthcare and education, where the greatest potential for discrimination may be lurking (PCAST, 2014). White House Advisors noted in healthcare big data that "large-scale analysis of research on disease, together with health data from electronic medical records and genomic information, might lead to better and timelier treatment for individuals, but also to inappropriate disqualification for insurance or jobs." The report also disclosed with regard to education that "knowledge of early performance can create implicit biases that color later instruction and counseling. There is great potential for misuse, ostensibly for the social good, in the massive ability to direct students into high- or low-potential tracks."(p. 14) The latter application of big data was likely a concern of the inBloom database parents and detractors—narrowing students' potential opportunities, possibly without their awareness, and certainly without consent.

4. BIG DATA AND PRIVACY: WHAT'S AN IT MANAGER TO DO?

Robert Zandoli, SVP and Global Chief Information Security Officer for AIG suggests that in order to protect privacy, the information systems manager should understand the life cycle of big data, which he separates into five phases:

- **Collection**–What kind of data is being collected? Is it reliable and secure?
- **Storage**–How is the data being stored? Where and with what type of protection?
- **Uses/Users**–How is the data being used and by whom?
- **Transfer**–How is the data being moved? Where is it going and is the transfer being done securely?
- **Destruction**–What are the data retention cycles? Who decides when to destroy the data and how will the destruction take place? (MIT Workshop, 2013).

In addition to the life cycle, individuals working in IS should also be familiar with the nature of privacy concerns. Steve Landefeld broke data privacy concerns into two groups in a paper presented at the UN sponsored 2014 *International Conference on Big Data for Official Statistics*:

Individual concerns are associated with "…disclosure of detailed personal medical, financial, legal or other sensitive information that would lead to discriminatory outcomes and uses for tax, investigation, legal and other government purposes." (2014, p. 15)

Business concerns are associated with the "…release of commercially valuable marketing and other data sets; propriety information on the methods and sources used to produce those data; disclosure to competitors of important strategic information on pricing, costs, profits, and markets; and the use of such information for tax, regulatory, investigation, legal and other purposes." (2014, p. 15-16)

Also important is the knowledge that analysis of big data compounds privacy issues as the phenomenon of data fusion brings additional privacy issues to the forefront. Individually, separate data streams may be adequately protected and kept confidential; however, when the streams are combined, emergent properties may present further privacy challenges (PCAST, 2014).

After IT personnel understand the way in which big data is managed and privacy concerns are categorized, they can address the issues of the indiscriminate or over-collection of big data, as well as the ever-present concerns about breaches of the systems intended to protect the collected information. The dual problem, then, for the information systems manager, is the collection of the appropriate data coupled with its security.

With regard to security of collected big data, it is important for information systems professionals to think not just in terms of cybersecurity when protecting privacy, but to focus their considerations on privacy policy and data use. Because even "if there were perfect cybersecurity, privacy would remain at risk. Violations of privacy are possible even when there is no failure in computer security. If an authorized individual chooses to misuse (e.g., disclose) data, what is violated is privacy policy, not security policy" (PCAST, 2014, p. 34).

Privacy Protection Methods

Therefore, to ensure the best protection for big data privacy in terms of collection, usage, and security, information technology students should be familiarized with current methods of protection. Beginning in 1996, the ISACA COBIT framework (Information Systems Audit and Control Association) (Control Objectives for Information and Related Technology) provided a comprehensive and systematic approach for managing and controlling information systems using a series of layered controls. COBIT 5 incorporates multiple frameworks including ISACA's Val IT (Value from IT Investments) and Risk IT, Information Technology Infrastructure Library (ITIL) and related International Organization for Standardization (ISO) standards (ISACA, 2015).

Another (previously mentioned) document that can provide guidance was created by The President's Council of Advisors on Science and Technology in 2014 entitled "Big Data and Privacy: A Technological Perspective" (PCAST, 2014). Both documents provide timely suggestions for privacy measures that can be incorporated throughout IS program coursework. Several of these privacy measures are described in Section 5, "Big Data and Privacy: A Layered Approach."

5. BIG DATA AND PRIVACY: INCORPORATING IT INTO THE CURRICULUM

The drive to produce graduates with big data skills is growing (Gorman & Klimberg, 2014). Gupta, Goul and Dinter (2015) recently described a model curriculum for Business Intelligence (BI) and Analytics electives. In developing their model, the authors surveyed IS faculty to determine the extent to which BI content was being implemented in classes. The authors found that Business Intelligence (BI) courses have gained relevance on campuses (Gorman & Klimberg, 2014) and that more departments offer

the courses as electives rather than as core courses (Gupta, Goul, & Dinter, 2015).

Gorman & Klimberg (2014) found that a majority of data analytics programs are found in business departments that combine Decision Sciences and Management Information Systems. However, not all colleges and universities are able to devote academic resources specifically for data analytics courses at this time. Instead, data analytics concepts and exercises are being incorporated into existing classes (Chen, Liu, Gallagher, Pailthorpe, Sadiq, et. al, 2012; Frydenberg, 2015). Thus, specific concepts, such as big data privacy protection may be skirted or overlooked. As future overseers of corporate data and information systems, it is important that IS students are not only aware of big data analytics, but that they also are familiar with keeping data private and using it appropriately. "Big data actually has a tremendous potential to solve some huge societal problems," stated FTC Commissioner Julie Brill at a recent Aspen Ideas Festival, [but] "I don't think any of these potential benefits are going to be realized until we solve the privacy issues." (Whiteman, 2014, para. 4).

IS2010 Curriculum Guidelines

In the Executive Summary of the IS 2010 Curriculum Guidelines, the authors note that the document's revision was shaped with the understanding that "… the curriculum reaches beyond the schools of business and management. "(p. vii) In addition, the document notes that the highest-level outcomes that the curriculum is expected to include are:

- Improving organization processes
- Exploiting opportunities created by technology innovations
- Understanding and addressing information requirements
- Designing and managing enterprise architecture
- Identifying and evaluating solution and sourcing alternatives
- Securing data and infrastructure, and
- Understanding, managing and controlling IT risks. (p. vii)

Thus, the framework was developed as a "living curriculum" that could adapt and transform to the changing environment. The dynamic nature of the model curriculum is especially valuable when you consider the expanding uses of big data in disciplines where privacy is essential, such as healthcare management. With that in mind, the next section describes how big data privacy concepts can be incorporated into the existing IS2010 Model Curriculum.

6. BIG DATA AND PRIVACY: A LAYERED APPROACH IN THE IS2010 MODEL CURRICULUM

Because protecting privacy in big data analytics is extremely important and there is a limited amount of resources (class time and faculty) to apply to teaching specific big data concepts, the authors suggest taking a cue from the COBIT model and applying a layered approach to covering big data privacy protection concepts throughout the Model Curriculum. In this section, the authors describe big data privacy concepts and suggest IS2010 courses (Table 1) in which concept coverage might be appropriate based upon the learning objectives of the course (Appendix).

IS2010.1	Foundations of IS
IS2010.2	Data and Information Management
IS2010.3	Enterprise Architecture
IS2010.4	Project Management*
IS2010.5	IT Infrastructure
IS2010.6	Systems Analysis and Design
IS2010.7	IS Strategy, Management, and Acquisition

Table 1. IS2010 Model Curriculum
* Big data privacy concepts were not suggested for incorporation into IS2010.4.

A culture of confidentiality needs to be fostered and reinforced by top level management and the organization's objectives. Employees should be regularly reminded of the company's stance on data privacy. (IS2010.1, 2, 3 & 7)

Reliable employees with proficient skills, clean background checks, and a history of honesty and integrity should only be allowed to access confidential data. (IS2010.2, 3 & 7)

A Data Governance Board can oversee the development, implementation, and adherence of data privacy policies. (IS2010.1, 2, 3, 6 & 7)

Written Policies and Procedures, specifically for big data access, storage, usage, confidentiality, governance, and policy violations, should be developed, signed, and accessible for employee review. Policy documents should be regularly updated and revised with employees commonly made aware of the policy changes. Employees should be asked to read and renew

their acceptance of updated privacy policies each year (IS2010.2, 3, 5, 6 & 7)

Physically protecting the data from unauthorized access through a layered approach of physical controls such as the choice of data storage locations, multiple locked doors, and human gatekeepers. (IS2010.2, 3, 5, 6 & 7)

Authorized and authenticated access to the data through logins and passwords, biometric controls and password policies. (IS2010.1, 2, 3, 5, 6 & 7)

Anonymization and De-identification methods are often used to mask the data provider's identity. However with the glut of available data, the benefits of these methods can easily be nullified (PCAST, 2014). (IS2010.2, 3, 5, 6 & 7)

Encryption and digital signatures are usually standard topics addressed in Introductory MIS textbooks. However, further discussion of those topics might include (1) end-to-end encryption and limiting the amount of time that data to be encrypted is stored in an unencrypted format, (2) limiting access to unencrypted data, (3) policies to ensure that confidential data is kept protected and private, (4) use of different types of encryption keys such as identity- or attribute-based encryption, and (5) recent developments for data privacy protection (PCAST, 2014). (IS2010.1, 2, 3, 5, 6 & 7)

Reduce exposure: In a report published by the Sans Institute regarding the Target credit card breach of 2013, the report indicates that the attackers might have used simple Google searches to conduct reconnaissance on Target. Information that the attackers could have easily found include material regarding Target's vendor portal and some of the vendors in which they interact, as well as a detailed case study describing Target's use of virtualization software, their technical infrastructure, detailed Point of Sale system information and information regarding their security patches and system updates deployment system (SANS, 2014).

In protecting data from leaking and systems from being breached, companies need to limit exposures and vulnerabilities and approach describing their systems and data structures on a "need to know basis." (IS2010.2, 3 & 7)

Differential Privacy and "Noising" techniques can be used to obfuscate the data and confuse the reader should the data be breached. (IS2010.2, 3. 5, 6 & 7)

Deletion and Non-Retention polices are beneficial, but not foolproof as data may be stored in multiple locations. Retained data streams can be stored separately in an anonymized and encrypted format on password protected storage. (IS2010.1, 2, 3, 5 & 7)

Notice and Consent provision at each point in the data collection process should be emphasized to distribute the privacy burden to the data providers. (IS2010.2, 3, 6 & 7)

Management of data access and usage logs should be handled on regular basis. Policies for handling observed issues and violations should be followed and strictly enforced. (IS2010.2, 3, 5 & 7)

A summary of the IS2010 course objectives and the big data privacy methods that could be addressed in those courses are outlined in the appendix. Due to time restrictions, faculty will want to select concepts from the list of those suggested.

7. CONCLUSIONS

Although privacy concepts have been addressed in IS courses, the need to emphasize those topics in light of rising data breaches and big data analytics is becoming increasingly apparent. Both The President's Council of Advisors on Science and Technology and ISACA's COBIT framework provide a detailed collection of data privacy measures that can be incorporated into coursework and applied in the field. However, incorporating privacy concepts into course material that is specific to big data analytics, is met with restrictions. In this paper, the authors propose a layered approach to addressing data privacy methods by incorporating multiple methods throughout the IS2010 Model Curriculum.

8. REFERENCES

Banerjee, U. (2013). Who coined the term Big Data? *Technology Trend Analysis Blog*. Retrieved June 10, 2015 from https://setandbma.wordpress.com/ 2013/02/04/who-coined-the-term-big-data/

Bogel, A. (2014). What the failure of inBloom means for the student-data industry. *Slate Future Tense News*. Retrieved June 10, 2015 from http://www.slate.com /blogs/future_

tense/2014/04/24/what_the_failure_of_inbloom_means_for_the_student_data_industry.html

Chen, L., Liu, Y., Gallagher, M., Pailthorpe, B., Sadiq, S., Shen, H. T., & Li, X. (2012). Introducing cloud computing topics in curricula. *Journal of Information Systems Education,23*(3), 315-324.

Craig, T., & Ludloff, M. (2011). *Privacy and Big Data*. O'Reilly Media, Sebastopol, California.

DataScience Series/Where Big Data Happens (2012). *Ten Practical Big Data benefits. Greenplum*. Retrieved June 10, 2015 from http://datascienceseries.com/stories/ten-practical-big-data-benefits.

Dell Press Release. (2014). Dell Survey: Midmarket companies aggressively embrace Big Data projects. *Dell Press Release*. Retrieved June 10, 2015 from http://www.dell.com/Learn/us/en/uscorp1/press-releases/2014-04-28-dell-software-big-data-midmarket-survey.

Ducher, J. (2014). What is Big Data? *DataScience@BerkeleyBlog*. Retrieved June 10, 2015 from http://datascience. Berkeley. edu/ what-is-big-data/.

Gorman, M. F., & Klimberg, R. K. (2014). Benchmarking academic programs in business analytics. *Interfaces, 44*(3), 329-341.

Gupta, B., Goul, M., & Dinter, C. (2015). Business Intelligence and Big Data in Higher Education: Status of a Multi-Year Model Curriculum Development Effort for Business School Undergraduates, MS Graduates, and MBAs. *Communications of the Association for Information Systems*, *36*(23), 449-476.

ISACA (2015). What is COBIT 5? *COBIT: An ISACA Framework*. Retrieved on June 13, 2015 from https://cobitonline.isaca.org/about.

Kamenetz, A. (2014). What will happen to 'Big Data' in education? Mind/Shift, *KQED News and National Public Radio (NPR*). Retrieved June 10, 2015 from http://ww2.kqed.org/mindshift/2014/04/03/.what-will-happen-to-big-data-in-education/.

Landefeld, S. (2014). Uses of Big Data for Official Statistics: Privacy, Incentives, Statistical Challenges, and Other Issues. *International Conference on Big Data for Official Statistics, United Nations Statistics Division and National Bureau of Statistics of China*, Retrieved June 12, 2015 from http://unstats.un.org/unsd/trade/events/2014/beijing/Steve%20Landefeld%20-%20Uses%20of%20Big%20Data%20for%20official%20statistics.pdf.

Madda, M.J. (2014). Where inBloom wilted. *edSurge Education Technology News*. Retrieved from https://www.edsurge.com/n/2014-02-05-where-inbloom-wilted.

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A. (2011). Big data: The next frontier for innovation, competition, and productivity. Retrieved June 11, 2015 from http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_forinnovation.

Massachusetts Institute of Technology (MIT) Big Data Initiative at CSAIL (2013). *Member Workshop #2: Big Data Privacy, Exploring the Future Role of Technology in Protecting Privacy*. Retrieved on June 12, 2015 from http://bigdata.csail.mit.edu/sites/sites/bigdata/files/u9/MITBigDataPrivacy_WKSHP_2013_finalvWEB.pdf.

President's Council of Advisors on Science and Technology (PCAST) (2014). Report to the President, *Big Data and Privacy: A Technological Perspective*. Retrieved on June 10, 2015 from https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_may2014.pdf.

President's Council of Advisors on Science and Technology (PCAST) (2015). Interim Report to the President, *Big Data: Seizing Opportunities, Preserving Values*. Retrieved June 12, 2015 from https://Whitehouse.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf.

Press, G. (2014). 12 Big Data Definitions What's Yours? *Forbes Tech News*. Retrieved June 12, 2015 from http://www.forbes.com/sites/gilpress/2014/09/03/12-big-datadefinitions-whats-yours.

Rubenstein, I. (2012). Big Data: The End of Privacy or a New Beginning? International Data Privacy Law, (Forthcoming), *NYU School of Law*, Public Law Research Paper No. 12-56.

Radichel, T and Northcutt. S. (2014). Case Study: Critical Controls that could have Prevented Target Breach. *SANS Institute InfoSec Reading Room*. Retrieved June 13, 2015 from http://www.sans.org/reading-

room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412.

Schrage, M. (2014). Big Data's dangerous new era of discrimination. *Harvard Business Review.* Retrieved June 10, 2015 from https://hbr.org/2014/01/big-data-dangerous-new-era-of-discrimination.

Simon, S. (2013). K-12 student database jazzes tech startups, spooks parents. *Reuters Technology News*. Retrieved June 10, 2015 from http://www.reuters. Com/article/2013/03/03/us-education-Database-idUSBRE92204W20130303.

Trippick, S. (2014). Information is the Oil of the 21st Century. Leverage It., *The Staffing Stream: The voices of the Staffing Industry*. Retrieved June 12, 2015 from http://www.thestaffingstream.com/2014/09/11/information-is-the-oil-of-the-21st-century/.

Tobin, P. (2013). Big Data brings four big risks. *Forbes Tech News*. Retrieved June 12, 2015 from http://forbes.com/sites /sungardas/2013/12/18/big-data-brings-four-risks.

Whiteman, M. (2014, July 3). What Big Data means for privacy. *The Aspen Institute Idea Blog*. Retrieved on June 12, 2015 from http://www.aspeninstitute.org/about/blog/what-big-data-means-privacy.

Editor's Note:

This paper was selected for inclusion in the journal as a EDSIGCon 2015 Distinguished Paper. The acceptance rate is typically 7% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2015.

Appendix

Core Curriculum	Learning Objective	Privacy Protection Measures
IS2010.1 Foundations of Information Systems	7. Mitigate risks as well as plan for and recover from disasters. 10. Understand how various types of IS provide the information needed to gain business intelligence to support the decision making for the different levels and functions of the organization. 11. Understand how enterprise systems foster stronger relationships with customers and suppliers and how these systems are widely used to enforce organizational structures and processes. 13. Understand how to secure information systems resources, focusing on both human and technological safeguards. 14. Evaluate the ethical concerns that information systems raise in society and the impact of information systems on crime, terrorism, and war.	• Culture of confidentiality • Data Governance Board • Physical protection • Authorized & authenticated access • Encryption & digital signatures • Deletion & non-retention policies
IS2010.2 Data and Information Management	3. Understand the basics of how data is physically stored and accessed. 17. Understand the key principles of data security and identify data security risk and violations in data management system design.	• Culture of confidentiality • Reliable employees • Data Governance Board • Written Policies & Procedures • Physical protection • Authorized & authenticated access • Anonymization & de-identification methods • Encryption & digital signatures • Reduce exposure • Differential privacy and "noising" techniques • Deletion & non-retention policies • Notice & consent • Management of data access & usage logs
IS2010.3 IS Enterprise Architecture	3. Utilize techniques for assessing and managing risk across the portfolio of the enterprise. 4. Understand the benefits and risks of service oriented architecture.	• Culture of confidentiality • Reliable employees • Data Governance Board • Written Policies & Procedures • Physical protection • Authorized & authenticated access • Anonymization & de-identification methods • Encryption & digital signatures • Reduce exposure

		• Differential privacy and "noising" techniques • Deletion & non-retention policies • Notice & consent • Management of data access & usage logs
IS2010.5 IT Infrastructure	2. Understand the principles of underlying layered systems architectures and their application to both computers and networks. 14. Analyze and understand the security and business continuity implications of IT infrastructure design solutions. 15. Configure simple infrastructure security solutions.	• Written Policies & Procedures • Physical protection • Authorized & authenticated access • Anonymization & de-identification methods • Encryption & digital signatures • Differential privacy and "noising" techniques • Deletion & non-retention policies • Management of data access & usage logs
IS2010.6 Systems Analysis and Design	11. Incorporate principles leading to high levels of security and user experience from the beginning of the systems development process. 13. Analyze and articulate ethical, cultural, and legal issues and their feasibilities among alternative solutions.	• Data Governance Board • Written Policies & Procedures • Physical protection • Authorized & authenticated access • Anonymization & de-identification methods • Encryption & digital signatures • Differential privacy and "noising" techniques • Notice & consent
IS2010.7 IS Strategy, Management, and Acquisition	1. Understand the various functions and activities within the information systems area, including the role of IT management and the CIO, structuring of IS management within an organization, and managing IS professionals with the firm. 2. View an organization through the lens of non-IT senior management in deciding how information systems enable core and supportive business. 8. Understand existing and emerging information technologies, the functions of IS and its impact on the organizational operations.	• Culture of confidentiality • Reliable employees • Data Governance Board • Written Policies & Procedures • Physical protection • Authorized & authenticated access • Anonymization & de-identification methods • Encryption & digital signatures • Reduce exposure • Differential privacy and "noising" techniques • Deletion & non-retention policies • Notice & consent • Management of data access & usage logs