: What decision support data should be anonymous, confidential, private?

by Daniel Power

Editor, DSSResources.com

Big data can mean big problems for individuals and organizations. Edward Snowden's NSA leaks demonstrate some of the problems of data privacy and security. Also, many people wrongly assume there is a **right** to privacy in the United States. Linder (2013) notes however that "the U. S. Constitution contains no express right to privacy." He does explore some implicit protections in the U.S. Constitution, but the framers of the U.S. Constitution did not and could not anticipate the rapidly evolving technology possibilities for collecting and analyzing data about people, their beliefs and behaviors. Organizations are collecting extensive data about individuals including customers, employees, and suppliers. More behavioral and unstructured data will be collected in the future and it will be analyzed.

We live in a digital, interconnected World. Most people can not be anonymous on the network. Confidential documents, click strokes and digital speech can be intercepted, stored and analyzed. Perhaps it is **un**reasonable to expect that what people say or do is anonymous, confidential or private in contemporary society. Businesses and governments have many methods for collecting data and the cost of methods like video cameras, radio frequency identifiers (RFID) and fingerprint recognition is declining rapidly.

Market researchers in companies want to know everything there is to know about customers and potential customers. Some managers in human resources what to know everything about individual employees. A few managers want to know about the private lives of managers in competing or supplier firms. Managers and actuaries in some auto insurance companies want to know about customer driving habits. Bank managers, law enforcement officers and private detectives want to catch criminals and identify fraud and other criminal activity. Managers in credit card companies want to identify bad credit risks, people who won't pay their debts. Retailers want to keep track of customer buying behavior to sell more products. This list of problematic data desires is only the beginning of a potentially much longer list.

In the United States, "The Health Insurance Portability and Accountability Act (HIPAA)has a Privacy Rule that attempts to provide "federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of health information needed for patient care and other important purposes(see http://www.hhs.gov/ocr/privacy/)". Unfortunately, the construction of these privacy rules have created new problems for patients and their families and may provide no real privacy despite the extremely high cost of administering HIPAA and its inconveniences. Bureaucratic laws don't safeguard privacy very effectively.

: What decision support data should be anonymous, confidential, private?

Professor Marc Rotenberg taught a course on Information Privacy Law at Georgetown University Law Center in Spring 2013. His syllabus is on the Internet at http://epic.org/misc/gulc/. Rotenberg asserts "Privacy is a fascinating and rapidly changing field." From my perspective, the legal issues seem complex and more historic than relevant to the challenges of modern data gathering and analysis. Anticipating problems and finding legal safeguards is an ongoing challenge.

From a business perspective, it may seem desirable that individuals should have **no** right to control or even know of personal information held by a company. Assuming the data comes from a primary or direct source and laws have been followed, then the data is the **property** of the company that gathered it. So when copyright or public privacy rules are not involved, any data gathered legally is arguably appropriate for decision support. One can assert that data is data and **all relevant** data should be used to inform business decisions.

Sadly, company data can be misused and misuse can create liabilities and problems for a company. When a company and its managers choose to capture and retain data, there is an implicit obligation created to guard and protect the data from unauthorized and inappropriate use. So companies need policies on how data should be protected, when data should be destroyed and when data should be anonymous. More data with greater access and new analytical capabilities mean there are more opportunities for data breach and abuse.

References

Lindner, D. "Exploring Constitutional Conflicts," 2013 at URL http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html

Author: Daniel Power
Last update: 2013-09-29 02:28