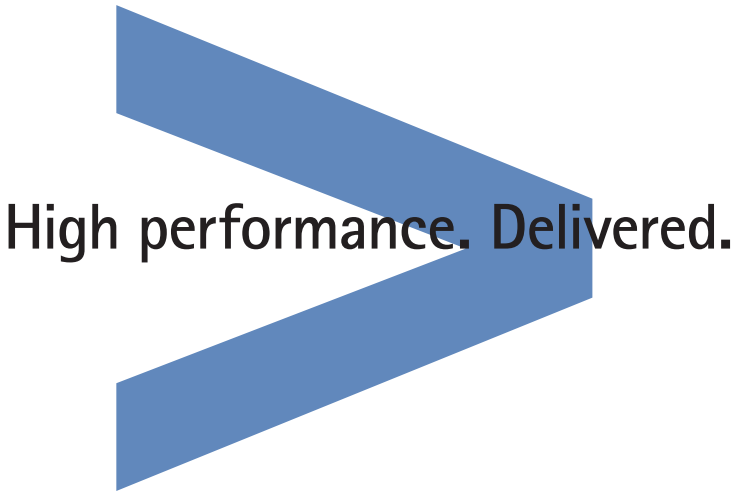
accenture

Strategy | Digital | Technology | Operations

Outlook

The online journal of high-performance business



Special Report | Accenture Technology Vision 2015

The case for data ethics

By Steven C. Tiell

At the core of all stakeholder relationships involving personal data is an extraordinary degree of trust. To win that trust, companies must go beyond privacy laws and existing data control measures to embrace practices and behaviors based on the highest ethical standards.

Personal data is the coin of the digital realm, which for business leaders creates a critical dilemma. Companies are being asked to gather more types of data faster than ever to maintain a competitive edge in the digital marketplace; at the same time, however, they are being asked to provide pervasive and granular control mechanisms over the use of that data throughout the data supply chain.

The stakes couldn't be higher. If organizations, or the platforms they use to deliver services, fail to secure personal data, they expose themselves to tremendous risk—from eroding brand value and the hard-won trust of established vendors and customers to ceding market share, from violating laws to costing top executives their jobs.

To distinguish their businesses in this marketplace, leaders should be asking themselves two questions. What are the appropriate standards and practices our company needs to have in place to govern the handling of data? And how can our company make strong data controls a value proposition for our employees, customers and partners?

Defining effective compliance activities to support legal and regulatory obligations can be a starting point. However, mere compliance with existing regulations—which are, for the most part, focused on privacy—is insufficient. Respect for privacy is a byproduct of high ethical standards, but it is only part of the picture. Companies need to embrace *data ethics*, an expansive set of practices and behaviors grounded in a moral framework for the betterment of a community (however defined).

Raising the bar

Why *ethics*? When communities of people—in this case, the business community at large—encounter new influences, the way they respond to and engage with those influences becomes the community's shared ethics. Individuals who behave in accordance with these community norms are said to be moral, and those who are exemplary are able to gain the trust of their community.

Over time, as ethical standards within a community shift, the bar for trustworthiness is raised on the assumption that participants in civil society must, at a minimum, adhere to the rule of law. And thus, to maintain moral authority and a high degree of trust, actors in a community must constantly evolve to adopt the highest ethical standards.

Actors in the big data community, where security and privacy are at the core of relationships with stakeholders, must adhere to a high ethical standard to gain this trust. This requires them to go beyond privacy law and existing data control measures. It will also reward those who practice strong ethical behaviors and a high degree of transparency at every stage of the data supply chain. The most successful actors will become the platform-based trust authorities, and others will depend on these platforms for disclosure, sharing and analytics of big data assets.

Data ethics becomes a value proposition only once controls and capabilities are in place to granularly manage data assets at scale throughout the data supply chain. It is also beneficial when a community shares the same

behavioral norms and taxonomy to describe the data itself, the ethical decision points along the data supply chain, and how those decisions lead to beneficial or harmful impacts.

A common language

Data scientists have already weighed in on the issue. Forty-two percent of respondents to a survey taken at the Joint Statistical Meeting's annual gathering in August 2014 agreed that ethical research standards should be in place for data scientists, while 43 percent said that ethics already plays "a big part" in their research.[1]

Specific ethical data practices need to be woven all through a company's cultural fabric.

Strong controls all along the data supply chain—collection, aggregation, sharing, analysis, monetization, storage and disposal—are paramount to success. As these practices spread, the benefits of having a common taxonomy to appropriately describe the classes of risk at each point along the data supply chain become increasingly important.

In cyber security, a classification system for 67 unique protection-motivated behaviors has been proposed to provide researchers and practitioners with a common nomenclature.[2] The benefits of a clear and common understanding of data ethics will help practitioners collaborate, regulators govern, and business owners appropriately manage the risk at each stage of the data supply chain.

To get to this enviable position, leaders must first accept data ethics as a business risk. Next, specific ethical data practices must be identified and defined. Finally, these practices need to be woven all through a company's cultural fabric and become part of its operational excellence.

Gartner analysts are already seeing motion on these fronts. By 2017, they expect that 25 percent of large enterprises will have a digital code of conduct, and by 2018, that fully half of business ethics violations will be caused by the improper use of big data analytics. Also by 2018, Gartner expects regulatory disclosures related to failures in the organizational information risk control environment to rise 50 percent.[3] The more businesses depend on data-driven partnerships, revenue streams and decision support, the more important auditable and enforceable ethical practices become. Employees and automated systems must be able to identify opportunities for ethical decisions throughout the data supply chain to properly manage this risk.

Billion-dollar lapse

Data security lapses are costly. For retailers that have experienced a security breach, 12 percent of their loyal customers say they have stopped shopping at that retailer, and 36 percent will shop at those retailers less frequently.[4] The dollar damages can be just as painful—more than $230 million in direct expenses in one high-profile example of mishandled customer data, a lapse that would ultimately knock more than $1 billion off the company's net earnings for the year.

The issue of data security has also become an important part of the national conversation. According to a recent study by TRUSTe, 45 percent

[1] "Data Scientists Want Big Data Ethics Standards," InformationWeek, September 17, 2014. http://www.informationweek.com/big-data/big-data-analytics/data-scientists-want-big-data-ethics-standards/d/d-id/1315798

[2] Posey, Clay and Roberts, Tom and Lowry, Paul Benjamin and Bennett, Becky and Courtney, James, "Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors." MIS Quarterly, Vol. 37(4), pp. 1189-1210, December 31, 2013. Available at SSRN: http://ssrn.com/abstract=2173642

[3] "100 Information and Analytics Predictions through 2020," Gartner, January 30, 2015. http://www.gartner.com/document/2974431/meter/charge

[4] Retail Perceptions, "Retail's Reality: Shopping Behavior After Security Breaches," June 2014. http://www.interactionsmarketing.com/retailperceptions/2014/06/retails-reality-shopping-behavior-after-security-breaches

of US citizens think online privacy is more important than national security.[5] The same study found that while 92 percent of US Internet users are concerned about online privacy, only a little more than half (55 percent) say they trust most companies with their personal information online, and 91 percent say they avoid companies that do not protect their privacy.

Adherence to ethical standards can amplify customer growth just as concerns about ethical practices can amplify attrition. Case in point: Threema, a secure messaging service for smartphones that offers end-to-end encryption, doubled its user base from 200,000 to 400,000 in the 24 hours after Facebook's acquisition of WhatsApp in February 2014.[6] As an independent company, WhatsApp had earned a high degree of trust among users that the service would protect the privacy of their communications. But once the company was acquired by Facebook, the WhatsApp community immediately identified with the privacy concerns of Facebook users.

The lesson: If the entity in question is a platform, the effects of lax ethical data practices are compounded and can ripple throughout systems—even more so if decision making is being performed by automated algorithms. These risks were shown in the Flash Crash of May 6, 2010, when the Dow Jones plunged 9 percent in two minutes caused by a confluence of systemic volatility with algorithmic trading organizations.[7] To the data ethicist, this event begs the question, "If autonomous trading algorithms were required to adhere to a stringent code of ethics, would this Flash Crash have been less severe or perhaps been prevented altogether?"

Nor are these issues confined to financial markets. Decision making by autonomous agents is of particular concern when seen in the context of the Internet of Things. As connected networks of small, embedded sensors become more pervasive, autonomous decision making is being pushed to the edge of networks, where the digital and physical worlds intersect.

At this intersection, sensors and analytical systems make autonomous decisions that affect the real world, such as real-time traffic management and responsive street-lighting systems. To protect public safety, these sense-and-respond systems must be governed by ethical algorithms. This is not alarmist. In 2014, a German steel plant suffered significant physical damage to production machines as the result of a cyberattack.[8]

Ethical handling of data must no longer be taken for granted. In the digital era, proper controls and policies for managing data throughout its supply chain are necessary for reducing business risks that can quickly impact the bottom line. A control framework to enable leaders to operate "ethically by design" needs to be established. In doing so, businesses can strike a balance between minimizing risk and seizing opportunities for value creation.

[5] "2015 TRUSTe US Consumer Confidence Index," TRUSTe.com, December 5, 2014 and January 12-15, 2015. http://www.truste.com/resources/privacy-research/us-consumer-confidence-index-2015/; "45 Percent Of Americans Think Online Privacy is More Important Than National Security," PRnewswire.com, January 28, 2015. http://www.prnewswire.com/news-releases/45-percent-of-americans-think-online-privacy-is-more-important-than-national-security-300026808.html

[6] "Verschlüsselte Nachrichten: WhatsApp-Alternative verdoppelt Nutzerzahl über Nacht," Spiegel Online, February 21, 2014. http://www.spiegel.de/netzwelt/apps/whatsapp-alternative-threema-verdoppelt-nutzerzahl-a-954915.html

[7] "Findings Regarding the Market Events of May 6, 2010," U.S. Securities and Exchange Commission, September 30, 2010. http://www.sec.gov/news/studies/2010/marketevents-report.pdf

[8] "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," Wired.com, January 8, 2015. http://www.wired.com/2015/01/german-steel-mill-hack-destruction/; "Cyberattack on German Steel Plant Caused Significant Damage: Report," Security Week, December 18, 2014. http://www.securityweek.com/cyberattack-german-steel-plant-causes-significant-damage-report

Robust data ethics is critical to the continued advancement of the digital business era. During the next three to five years, the big data community will see the emergence of trusted brokers acting as arbitrageurs in the big data marketplace. This opportunity to transform the way data is acquired, shared and used can happen only if the bar for trust is set high enough to guarantee sufficient security, privacy and transparency for all of the participants, not only in the big data community but in the economy as well. ■

About the authors

Steven Tiell is director of the Accenture Technology Vision. He is based in San Francisco, California. *steven.c.tiell@accenture.com*

The author would like to thank **David M. Cooper** and **Richard Bartley** (Accenture Security Strategy, Risk Management and Transformation practice), **Karen Swanson** (Accenture Research), **Hallie Benjamin** (Accenture Technology Labs), **Lucy Bernholz** (Center for Philanthropy and Civil Society, Stanford University), **David Gutelius** (The Data Guild) and **William Hoffman** (World Economic Forum) for their contributions to this article.

Outlook is published by Accenture.