Big Data: Big benefits and imperiled privacy

How data analytics is transforming how we live and work—and impacting personal privacy
Increasingly, our world is informed by Big Data

Data analytics has become a powerful force for change, one that can be used to benefit individuals, businesses, and government. Big Data has risen to the fore, in part, because it has become progressively less expensive to collect, store, and analyze information. At the same time, new sources of data—sensors, cameras, and mobile devices, to name but a few—continue to infiltrate business operations and personal lives and are generating an unprecedented volume of information.

This explosion of data collection and almost-instant analysis has elevated the issue of personal privacy to a matter of public debate. That’s because while Big Data promises profound benefits, the potential threats to personal privacy are simply too great to ignore. To address this, the White House in May published two high-profile studies of the potential impact of Big Data on personal privacy. The Podesta study concludes with six policy recommendations, including a renewed call to advance the Consumer Privacy Bill of Rights and a national data-breach standard.

A parallel report, titled “Big Data and Privacy: A Technological Perspective,” explores the current and future technologies for managing and analyzing data, and the implications of these technologies on public policy designed to protect privacy of personal data. It was published by the President’s Council of Advisors on Science and Technology (PCAST), an advisory group that includes scientists, engineers, academics, and industry representatives.

We took a detailed look at the security and privacy aspects of both studies to understand the likely policy implications, the potential impacts to cybersecurity and privacy, and the strategic steps organizations should take to adopt Big Data.

The Podesta study offers scenarios that demonstrate how Big Data analytics can help governments improve healthcare, education, homeland security, and law enforcement. Many of its policy recommendations—including adoption of the Consumer Privacy Bill of Rights and national data-breach legislation—echo proposals by the Obama Administration’s February 2012 Consumer Data Privacy Framework and its 2011 Cybersecurity Legislative Proposal.

The PCAST report describes a handful of scenarios that forecast how technologies will impact healthcare and education, in particular, as well as potential negative consequences such as biases in civil rights and discrimination based on personal information. It concludes with five general recommendations that center on the technical feasibility of broad policy approaches.

1 Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values, May 2014
2 Executive Office of the President, Big Data and Privacy: A Technological Perspective, May 2014
A unique proposal to standardize consumer privacy profiles

Both reports advance new technological proposals that could change the debate on how data privacy is defined and enforced.

The PCAST study recommends that privacy policy focus on how Big Data is used, rather than what data is collected or how it is gathered.

The Podesta report describes data as “dual use,” meaning that the contextual use of data can be either beneficial or harmful. It recommends adoption of advanced data-tagging schemes—similar to those already employed by the Department of Homeland Security (DHS)—to encode details about the context of data collection and uses that have been approved by the consumer. This permission-based metadata would travel with the information to help ensure that the data is used only for the context it was collected. For instance, information about consumers collected during online shopping could not be used in an employment context. Individuals would be responsible for reviewing and agreeing to “notice and consent” agreements that govern the sharing their data.

The PCAST study echoes metadata concepts that are laid out by the Podesta report. It also underscores the inadequacy of current online consent agreements, noting that: “Only in some fantasy world do users actually read these notices and understand their implications before clicking to give their consent.” The PCAST report also argues that these consent agreements do not cover all potential uses of data by third parties.

The PCAST authors propose an intriguing solution: They suggest that organizations create a standard set of “privacy preference profiles” and allow individuals to choose the privacy profile they prefer. As an example, the PCAST study notes that one person might select a profile offered by a civil liberties foundation while another might select one created by a consumer-product reviews organization. Forward-looking companies that embrace this approach would vet online services or mobile apps to confirm that the product’s privacy and data-use notice are acceptable to consumers.

We believe this may represent an opportunity for some businesses, particularly in the retail and consumer products sector, to provide a differentiating service for their customers. It also could help build trust among consumers and improve the overall customer-experience strategy.

Privacy preference profiles would not be without challenges, however. Businesses will be required to manage these profiles over time and across their data and apps ecosystems, as well as those of their partners. This may prove particularly arduous for companies that have multiple partners and a range of privacy profiles for individual customers. Indeed, mediation across preference profiles could be a massive undertaking, one that could lead to second-order privacy challenges.

A focus on outcomes, not technology

Both studies note that technology advances have made many privacy and data-protection laws obsolete.

Consider, for instance, that the legal concept of personal privacy changed dramatically with the advent of home Wi-Fi and appliances that transmit personal data across the Internet and store this information in the cloud. The Podesta report recommends regulations that encourage the responsible use of data and privacy protection, no matter what technology is used to collect the information.

For technology companies, this may represent an opportunity to develop solutions that

---

3 Executive Office of the President, Big Data and Privacy: A Technological Perspective, May 2014
automate privacy protections across a broad spectrum of Big Data applications. What’s more, as consumers increasingly rely on digital technologies for more daily activities, businesses may find themselves in a position to demonstrate how they can exchange personal data for value. Doing so could provide a strategic relationship-building opportunity for companies that can assure customers that their data is protected from unauthorized access or use.

Harmonizing data privacy laws

The Podesta study’s call for national cyberbreach legislation, in addition to a related recommendation that non-US persons be granted the same privacy rights as US citizens, could result in significant progress toward harmonizing international privacy and cyberbreach standards.

The European Union (EU) follows a different approach to privacy protection, one that generally requires across-the-board rules for explicit consent on the use of an individual’s data. US-based companies with multiple business and product lines spread across geographic boundaries face significant challenges in determining the appropriate data-privacy controls. For retail and consumer and financial services companies in particular, protecting the privacy of customers who are EU citizens is an additional complexity.

The call for national cyberbreach legislation could result in significant progress toward harmonizing international privacy and cyberbreach standards.

The PCAST authors highlight the need for greater investment in automation and harmonization of privacy protection. They advocate the use of Big Data to analyze data and develop tools to assess national, state, regional, and international rules and regulations for inconsistencies and recommended controls. Companies that proactively develop this type of technology will very likely have a ready market among government agencies looking to define new privacy regulations. Other potential customers may include companies seeking to reduce risks while customizing goods and services for various geographic markets.

Using Big Data to forecast the future

To better understand the potential rewards and risks that Big Data poses to an individual’s privacy, the PCAST authors lay out future scenarios across a number of industries.

In healthcare, for example, the authors note that Big Data can help detect disease by analyzing millions of patient records, genomic information, and postings to social media. It also can help identify individuals who may be susceptible to a particular disease—and thereby play a role in preventative healthcare.

In education, the PCAST study discusses how data gleaned from online education courses could deliver instant feedback on learning styles and behaviors to customize course content and help individuals realize their full educational—and professional—potential. The authors point out that this data also can be used to improve education overall and to better understand the age at which children should be taught certain skills to improve adult performance in key areas.

PCAST also notes that these types of data analysis could be misused and result in privacy violations. Lacking adequate controls and protections, the ability to predict the probability of contracting a disease or failing a course could lead to future discrimination and create biases.

The use of data to predict future events is nothing new, however. Governments and businesses have long used data modeling to forecast scenarios and the uncertainties that may accompany these outcomes. The oil and gas industry, for instance, successfully employs future scenario-building to assess global resource scarcity and the political and social drivers that drive energy consumption.
The difference is that Big Data can provide a much more accurate and specific prediction, and companies that harness it to perform scenario modeling stand to gain real competitive advantages. For example, organizations that leverage future scenarios around Big Data applications for pharmaceutical development in Europe or “green” energy-transportation solutions in Asia may be better prepared to take advantage of upcoming trends and develop targeted technology applications in advance of their competitors.

How to integrate Big Data and privacy into the business strategy

The Podesta study emphasizes the transformational potential of Big Data and underscores how the “volume, variety, and velocity” of information are redefining many aspects of government, commerce, and private life. While the US government is just now beginning to address the intersection of Big Data and privacy, the regulations and laws to protect privacy and prevent misuse of information are not yet in sync with the transmutable scope and speed of data trends.

Nonetheless, the new White House studies underscore the importance of integrating a strategy for Big Data security and consumer privacy to gain and maintain competitive advantages. Organizations that adopt Big Data early on will be better prepared to grow their business and understand their customers while reducing costs and controls.

Doing so will demand that businesses develop a strategy that is built upon a trusting relationship with customers and integrates threat-informed cybersecurity and privacy policies with the overall corporate strategy. A strong cybersecurity strategy, for instance, should fuse proactive cyber-threat detection and incident-response capabilities with strong controls governing the collection, storage, use, and sharing of personal data. An organization’s multiple products, operating units, and geographic operating models will all impact and inform cybersecurity and privacy safeguards.

At a more tactical level, a Big Data strategy should be designed according to the company’s competitive environment, business operating model, and existing internal capabilities. This type of customization will require that organizations:

- Identify the organizational “owner” of Big Data strategy. This owner should have knowledge of privacy, security, anti-discrimination, and fit-for-purpose decisions related to Big Data collection, analysis, and use.

The Podesta study singles out healthcare as a sector that is rich in opportunities—as well as risks to security, privacy, and discrimination.

Data, the report notes, has long been a key tool in health industries. What’s new is how “born digital” healthcare data—information that it is created specifically for digital use by a computer or other digital system—can dramatically increase the speed and accuracy of patient diagnosis and treatment.

Consider, for instance, the emerging practice of predictive medicine. This new model of healthcare can help consumers maintain good health by identifying the right diet, exercise, and preventative care. It also can enable physicians to use data to project the spread of infectious diseases, as well as predict what diseases an individual is likely to contract and how he or she might respond to specific treatments.

Yet the medical data necessary to predict these future outcomes, in many cases, is considered private and is protected by a hodgepodge of conflicting state and federal regulations. In a world powered by Big Data, the Podesta report notes that it will be necessary to create data-use authorities to help realize potential healthcare gains while protecting consumer privacy. A key component will be a thorough re-evaluation of how patient information is shared with third-party healthcare partners.

The Podesta study notes that inappropriate use of patient data could not only violate privacy regulations, but also lead to discriminatory practices and circumvention of civil rights protections. Health insurers, for instance, could employ Big Data analytics to “digitally redline” unwanted groups. Similar concerns exist in education, housing, employment, homeland security, and law enforcement.

Ensuring appropriate data privacy practices among healthcare and insurance entities is likely to be a complex initiative. But health industry firms that leverage the power of Big Data and address these issues early on stand to gain distinct advantages.

Checking up on Big Data challenges and opportunities in health industries

The Podesta study notes that inappropriate use of patient data could not only violate privacy regulations, but also lead to discriminatory practices and circumvention of civil rights protections. Health insurers, for instance, could employ Big Data analytics to “digitally redline” unwanted groups. Similar concerns exist in education, housing, employment, homeland security, and law enforcement.

Ensuring appropriate data privacy practices among healthcare and insurance entities is likely to be a complex initiative. But health industry firms that leverage the power of Big Data and address these issues early on stand to gain distinct advantages.

Ensuring appropriate data privacy practices among healthcare and insurance entities is likely to be a complex initiative. But health industry firms that leverage the power of Big Data and address these issues early on stand to gain distinct advantages.
Companies with an integrated strategy for Big Data and privacy may be in a strong position to influence future industry, government, and national standards.

- Recruit, train, and retain top talent, including business experts who can strategically identify the best uses of Big Data and technical personnel to manage the data systems and analytic tools.
- Create and communicate a campaign to establish and promote a data-driven business culture.

A customized privacy strategy will be central to enhancing Big Data applications and helping prevent inappropriate use or leakage of data. As the US government builds and revises privacy standards in the era of Big Data, it is looking to the private sector for input and recommendations. Companies with an integrated strategy for Big Data and privacy may be in a strong position to influence future industry, government, and national standards. Developing a privacy strategy will demand that organizations:
- Design privacy controls that fit its business objectives, customer expectations, and regulatory requirements.
- Develop and maintain an accurate inventory of customer and employee data, applying the same level of rigor used to inventory financial and physical assets.
- Support privacy policies with appropriate operational controls.
- Vet third-party partners to help ensure they understand and meet privacy requirements.

---

**Four factors that will drive Big Data and privacy protections**

**Laws and regulation:**
When state and national governments harmonize and enforce privacy and data-breach laws and regulations, organizations will likely be inspired to report data breaches and share cybersecurity information without fear of penalty or litigation. Organizations should be encouraged to adopt new approaches to cyber-breach notifications, reasonable-use policies, and cybersecurity information sharing.

**Technology:** Implementing automated privacy profiles across multiple sectors could help ensure that organization-sponsored personal privacy profiles are accessible and adopted by consumers. Ease of use for customers across shopping channels, as well as genuine advances over current “notice and consent” systems, will be key. Commercial incentives from national and international bodies to invest in new privacy protection technologies could prove useful.

**Openness of the Internet:**
Debates over the future of Big Data are based on a common assumption: The Internet will remain a series of open networks through which data easily flows. Some countries have begun to harden their Internet systems, and the concept of net neutrality is uncertain. If the Internet becomes a network of closed networks, or “walled gardens,” the full potential of Big Data may not be realized.

**Regional innovation:**
Innovations in technological privacy protections in Asia and Africa may leapfrog Big Data analytics used in the US and Europe. The growing populations of Asia and Africa rely heavily on mobile technology for commerce and trade, and innovations in these areas could accelerate. Advances in digital payments, for instance, could provide new opportunities for adversaries to target and exploit payment systems.
Contacts

To have a deeper conversation, please contact:

**David Burg**
Principal, US & Global Cybersecurity Leader
david.b.burg@us.pwc.com

**Michael Compton**
Principal, Cybersecurity Strategy & Operations
michael.d.compton@us.pwc.com

**Peter Harries**
Principal, Health Industries
peter.harries@us.pwc.com

**John Hunt**
Principal, Public Sector
john.d.hunt@us.pwc.com

**Mark Lobel**
Principal, Technology, Information, Communications and Entertainment
mark.a.lobel@us.pwc.com

**Gary Loveland**
Principal, Consumer and Industrial Products & Services
gary.loveland@us.pwc.com

**Joe Nocera**
Principal, Financial Services
joseph.nocera@us.pwc.com

**Dave Roath**
Partner, Risk Assurance
david.roath@us.pwc.com

**Contributing authors:**

**Neelkamal Agarwal**
Director
neelkamal.agarwal@us.pwc.com

**Ramesh Nair**
Strategy& Vice President
ramesh.nair@strategyand.pwc.com

**Anand Rao**
Principal
anand.s.rao@us.pwc.com

**Laurie Schive**
Director
laurie.a.schive@us.pwc.com

**Craig Stronberg**
Director
craig.d.stronberg@us.pwc.com