McDermott Will & Emery

The New Normal: Big Data Comes of Age

May 12, 2014

SPECIAL REPORT

McDermott Will & Emery

SPECIAL REPORT

For more information, please contact your regular McDermott lawyer, or:

Heather Egan Sussman
+1 617 535 4177
hsussman@mwe.com

Jennifer S. Geetter
+1 202 756 8205
jgeetter@mwe.com

Scott Weinstein
+1 202 756 8671
sweinstein@mwe.com

Stephen W. Bernstein
+1 617 535 4062
sbernstein@mwe.com

Daniel Gottlieb
+1 312 984 6471
dgottlieb@mwe.com

Anne Marie Turner
+1 202 756 8800
amturner@mwe.com

Karen S. Sealander
+1 202 756 8024
ksealander@mwe.com

Julia Jacobson
+1 617 535 3881
jjacobson@mwe.com

Ann Killilea
+1 617 535 3933
akillilea@mwe.com

For more information about McDermott Will & Emery visit www.mwe.com

Table of Contents

10 The New Normal: Big Data Comes of Age

On May 1, 2014, the White House released two reports addressing the public policy implications of the proliferation of big data. The first report is by the Executive Office of the President, entitled "Big Data: Seizing Opportunities, Preserving Values," (White House Report) and relies, in part, on the second report, prepared by the President's Council of Advisors on Science and Technology (PCAST), entitled "Big Data and Privacy: A Technological Perspective" (PCAST Report).

While the Reports seem to ask more questions than they answer, taken together, they redirect the public policy narrative from "if" big data to "how" big data. Rather than trying to slow the accumulation of data or place (likely ineffective) barriers on its use in analytic endeavors, these Reports assert that we should acknowledge this "new normal" and focus on envisioning policy initiatives and legal frameworks that foster innovation, promote the exchange of information and support public policy goals, while limiting harm to individuals and society.

This article provides an overview of the two Reports, puts into context their conclusions and recommendations, and extracts key takeaways for businesses grappling with understanding what these reports—and this "new normal"—mean for them.

Background on the Reports

The two Reports, released simultaneously on May 1, 2014, conclude a 90-day study by the White House on big data, announced by President Obama during a January 17, 2014, speech on signals intelligence. The President tasked his Counselor, John Podesta to "look how the challenges inherent in big data are being confronted by both the public and private sectors; whether we can forge intentional norms on how to manage this data; and how we can continue to promote the free flow of information in ways that are consistent with both privacy and security."

Podesta convened a working group of senior administration officials, which held briefings with hundreds of stakeholders from industry, academia, civil society, government, civil liberties advocates, international data protection authorities, and practitioners in the health care, financial and information services industries. The working group also sponsored three conferences at universities and invited public comments through the *Federal Register* and the whitehouse.gov platform.

Executive Summary of the PCAST Report

Parallel to Podesta's working group efforts, PCAST prepared its Report, which provides technical guidance on big data information technology and the privacy challenges presented by collecting, storing and leveraging big data assets. PCAST was tasked with studying the "technological aspects of the intersection of big data with individual privacy" in both current and future states of technological capability.

DIGITAL DATA, ANALOG DATA AND DATA FUSION

The PCAST Report approaches its task by offering examples of the current collection and use of data that is "born digital" (*i.e.*, created for use specifically for a computer or digital processing system, such as e-mail) and "born analog" (*i.e.*, created from characteristics of the physical world captured in digital form, such as faces or voices through sensors such as cameras or recording devices). The PCAST Report notes that born analog data may require different considerations than born digital data, because sensors must have the ability to collect and read as much information as possible in order to be effective.

For data that is born digital, the PCAST Report identifies two potential privacy concerns: the "obvious" concern of over-collection and the "more subtle" concern known as "data fusion." Over-collection happens when engineering or device design causes the collection of data unrelated to the stated purpose. Examples of over-collection and related privacy concerns include social networking apps that clandestinely collect a user's contact list and then spam contacts with advertisements for the app. Data fusion, by contrast, "occurs

when data from different sources are brought into contact and new, often unexpected, phenomena emerge." This can happen through modern practices of data mining and pattern recognition, and when common identifying data are brought together from diverse sets. The privacy challenge in the case of data fusion is how to apply traditional frameworks, such as "notice and consent," when data fusion often happens in unexpected ways, with unexpected results. The PCAST Report does not attempt to advise how to solve this privacy challenge, but rather notes that this must be a priority going forward.

Against the backdrop of these privacy concerns, the PCAST Report makes four key conclusions about the sufficiency and relevance of available principles, best practices, technologies and policy levers for protecting privacy in the era of big data collection.

- First, the PCAST Report cautions that encryption is not a perfect solution for securing big data, but notes that it could be a valuable component in a comprehensive privacy solution. To demonstrate the privacy-facing nature of encryption, the report describes future encryption technologies that would allow for various forms of limited access to information based on the identity or attributes of the person seeking access to the data. Importantly, the Report acknowledges that many of these encryption techniques are in the early phases of development and are not ready to be implemented.
- Second, the PCAST Report discusses the potentially fatal limitations of the traditional "notice and consent" framework for information collection in an age of big data. It calls this approach unrealistic because it puts the burden on the individual to decide whether data holders are appropriately collecting and using their data based on lengthy descriptions of their policies. The report also concludes that notice and consent cannot accurately account for all of the potential downstream beneficial future uses. In addition, the Report points to the Federal Trade Commission (FTC) enforcement action involving the Brightest Flashlight Free app and its 50 million downloads to illustrate the limitations of our existing privacy legal framework. The app collected location data every time the flashlight was used and transmitted the data to its vendor. The Report comments that had the app disclosed this practice in its privacy policy, "which no one would have actually read, [this disclosure] would likely have forestalled any FTC action without much affecting the number of downloads."
- Third, the PCAST Report points out that anonymization and de-identification, at least as traditionally understood and defined, have limited relevance in the era of big data. The concepts are binary; data is or is not anonymized or de-identified. Identifiability in a big data environment may be better understood as being on a spectrum—each data point may not be linkable to a person, but as these data points are linked to one another, the data takes on other attributes of identifiability. Like dots in a pointillist painting, the importance of each data point is informed by its proximity and relation to other data dots, and from the aggregate of such dots a picture of an individual emerges (a concept often referred to as the "mosaic effect").
- Fourth, the PCAST Report is skeptical that data deletion and non-retention policies are effective means of protecting individual privacy for two reasons. It argues that excessive non-retention policies might undermine or even defeat the economic and social value in analyzing these datasets in future. It is also skeptical of technologies that allow for information to be viewed but not archived, as it points to instances where these technologies have been defeated by hackers and applications that take snapshots of the information before it is deleted.

So where does PCAST recommend we go from here? It is important to note that despite its disapproval of structuring big data privacy compliance efforts on traditional models of notice and consent, the PCAST Report still sees a role for consumer input in the collection of their information. PCAST envisions the creation of various privacy profiles, which would generally describe the preferences of individual consumers on the collection and use of information. These profiles could be generated and put into computable language by trusted third parties that have the resources to examine the growing uses for data and modify the profiles going forward. Consumers would need to select a profile, and data holders would be required to differentiate the way they use the data they collect

based on the different privacy categories selected by individual consumers.

PCAST also envisions the use of metadata to track information through the data life cycle to provide accountability if individuals are harmed by improper analysis or misuse of the data. PCAST advocates for states and the federal government to revisit privacy tort law and legal precedents to handle the new harms that can be caused by big data analysis, such as the loss of credit or ability to obtain a lease as a result of any misclassification based on big data analysis.

The PCAST Report concludes with five recommendations:

- Policy attention should focus more on the actual downstream uses of big data and less on its collection and analysis.
- Policies and regulation, at all levels of government, should not embed particular technological solutions, but rather should be stated in terms of intended outcomes. In other words, to avoid falling behind the technology, it is essential that policy concerning privacy protection should address the purpose (the what) rather than the mechanism (the how).
- With coordination and encouragement from the Office of Science and Technology Policy (OSTP) and the National Coordination Office for Networking and Information Technology Research and Development, agencies should strengthen U.S. research in privacy-related technologies and in the relevant areas of social science that inform the successful application of these technologies.
- OSTP, together with the appropriate education institutions and professional societies, should encourage increased education and training opportunities concerning privacy protection, including professional career paths.
- The United States should take the lead both in the international arena and at home by adopting policies that stimulate the use of practical privacy-protecting technologies that exist today. The United States can exhibit leadership both by its convening power (for instance, by promoting the creation and adoption of standards) and also by its procurement practices (such as its use of privacy-preserving cloud services).

PCAST provided a draft of its report to Podesta's working group, and the PCAST Report's findings and recommendations inform and underpin the technology discussion and conclusions drawn by the White House Report.

Executive Summary of the White House Report

The White House Report establishes its support for big data at the outset by reviewing how data analytics have been used historically for the betterment of communities and society. After pointing out past societal and economic benefits of data collection and analysis, the Report notes that "the collection, storage and analysis of data is on an upward seemingly unbounded trajectory" fueled by faster processing, cheaper storage and a growing number of data capture mechanisms in everyday products. As a result, the Report concludes that we live in a world of "near-ubiquitous data collection." From the get-go, the Report makes clear that it believes the case for the value of big data analytics has been established and that any constructive dialogue going forward should be on how to allow big data analytics to proceed unimpeded while still protecting privacy and other important values. The White House Report makes clear that the administration is committed to the ongoing role of big data in government endeavors and in the private sector.

The Report sidesteps any precise definition of big data and develops a definition based on effect—big data is distinguished by what it can do that other digital assets cannot. Although it notes that different people may define the term somewhat differently, the White House Report describes the common big data themes as the three V's: volume, variety and velocity. In other words, big data is "data that is so large in volume, so diverse in variety or moving with such velocity, that traditional modes of data capture and analysis are insufficient."

PRIVACY CHALLENGES OF BIG DATA

The White House Report acknowledges that the seemingly unlimited future potential uses of accumulated data raise

critically important questions as to "whether our legal, ethical and social norms are sufficient to protect privacy and other values in a big data world." The White House Report acknowledges the privacy challenges presented by the increasing collection and use of information, and seeks to begin the process of addressing these issues.

As a result, the White House Report conceives of itself as an exercise in issue spotting, to pose questions about "the relationship between individuals and those who collect data about them." Although the White House Report does not say so explicitly, its observations and recommendations almost suggest that the very concept of what it means for something to be private must be developed. The image of privacy that emerges is less one of *secrecy* and more one of *regulated rules of conduct*.

In particular, the White House Report proposes six policy recommendations to promote the responsible and accountable use and disclosure of big data:

- **Advance the Consumer Privacy Bill of Rights**. A recommendation that the U.S. Department of Commerce seek to promote the "responsible use" of big data through the advancement of industry-developed "codes of conduct" in line with the Fair Information Practice Principles.
- **Pass national data breach legislation**. A request for Congress to pass a national standard for breach notification that includes reasonable time periods for notification of individuals affected, minimizes interference with law enforcement investigations, and prioritizes notification for large, harmful incidents over smaller ones.
- **Expand privacy protections to non-U.S. persons**. A recommendation for the Office of Management and Budget to work with agencies to apply the Privacy Act of 1974 to non-U.S. persons, or to establish alternative privacy policies that apply regardless of a person's nationality.
- **Ensure data collected on students in school is used for educational purposes**. A recommendation for government agencies to revisit the Family Educational Rights and Privacy Act regulations and the Children's Online Privacy Protection Act regulations to ensure that students in school are protected from inappropriate uses of educational data, while still allowing for such data to be used to improve educational approaches through new methods and business models.
- **Expand technical expertise to stop discrimination**. A recommendation that the U.S. Department of Justice and other government agency protectors of civil rights develop new ways to analyze big data to detect and investigate discrimination.
- **Amend the Electronic Communications Privacy Act (ECPA)**. A request that Congress pass legislation to modernize ECPA, ensuring that electronic data is afforded protections consistent with those afforded to physical items, including a recommendation to reassess the current availability of message metadata for law enforcement and third-party viewing.

Concepts at a Crossroads – Important Concepts to Watch

While much of the White House Report is geared for public consumption and is not controversial, it does touch upon some challenging issues and raise some provocative suggestions that, to certain audiences, will be significant. These warrant careful consideration, as they are likely to be among the contested issues in the ongoing dialogue about the role of data collection and analytics in the big data world.

NOTICE AND CONSENT

The White House Report notes that the notice and consent model—in which data subjects are informed about the potential uses of their data and must give their consent to such uses—forms the basis of much of the current privacy and security compliance framework. This model is predicated on there being a meaningful opportunity and means to provide notice, and an informed process to negotiate consent or decline. The White House Report, however, indicates its concern that the "notice and consent" framework is no longer the gold standard, or even a particularly relevant standard, in the modern digital economy. The Report notes, for example, concerns about "privacy policy fatigue" following which

individuals no longer take the time to read the countless privacy policies with which they are presented. Also, the White House Report, noting that big data analytics necessarily involves vast quantities of data, questions whether it is realistic for users to consent up front for each and every current and future use of their data.

The White House Report suggests that the regulation of big data might be better anchored by a focus on responsible use and accountability. The administration's first policy recommendation directs the Department of Commerce to seek comment on how the Consumer Privacy Bill of Rights developed by the administration could support these policy goals. Based on these comments, one likely outcome of these reports is that the administration may seek industry participation in the development of further codes of conduct that focus specifically on these two principles of notice and choice, similar to the process undertaken in 2013 by the Department of Commerce and its multi-stakeholder process involving mobile transparency.

Under such a "code of conduct" framework, companies in specific industries, such as health, financial services, social media and internet advertising, may be called upon to agree on limitations to the ways they can use and disclose consumer information within their industry. These limitations could be memorialized in "codes of conduct" to which industry members could voluntarily agree. If given the additional authority by Congress, the FTC could then approve or disapprove these codes and actively enforce their requirements.

A PREFERENCE FOR SECTORAL PRIVACY APPROACH

The White House Report expresses a preference for the United States' sectoral approach to privacy as opposed to the European Union's generally applicable privacy standards that recognize privacy as a fundamental human right. While noting that the U.S. approach sometimes leaves gaps for information that falls between sectors, particularly health information (which may not clearly fall under the Health Insurance Portability and Accountability Act (HIPAA) or the FTC Act or any other law), the White House Report argues that the U.S. approach gives industry more room to innovate.

The Report's preference for shifting focus from limiting collection to "responsible use" also creates tension with the EU approach, which puts significant emphasis on the concept of "data minimization" and promoting consumer choice about uses at the time data is collected. These tensions may be addressed during ongoing negotiations between the United States and Europe concerning the U.S.-EU Safe Harbor Framework, and we will continue to watch for developments in those talks.

IMPACT TO HEALTH CARE AND LIFE SCIENCE INDUSTRIES

The health and life sciences sectors, as noted in the White House Report, increasingly turn to big data analytics to drive innovation, control costs and enhance quality. The Reports contain a number of potential early signs of privacy policy redirection. For example, in general, the White House Report focuses on the positives of an industry sector approach to privacy. However, the Report expresses concern that the regulatory scope of HIPAA, currently limited to health care providers, health plans, and health care clearinghouses and their business associates, may not be sufficiently wide to capture the proliferation of entities that collect personal information from consumers through mobile apps and web-based solutions. This concern suggests that the FTC or other federal regulators may seek to fill the gap.

The White House Report also notes the blurry line between health information and non-health information under existing laws where the "health" quality of the information may depend on the disclosing or receiving party's status, rather than on the content of the information. The White House Report indicates that new or amended federal privacy legislation may be necessary, so recommendations for additional legislation may be coming.

As noted above, the White House Report also concludes that de-identification may be impossible in the era of big data, or may need a fundamentally revised definition. If this paradigm shift occurs, it would have a significant impact on research laws and regulations and research design, because most federal and state research laws assume that information is either identifiable or non-identifiable, and this distinction determines whether the research is subject to heightened regulation.

THE ADVERTISING-SUPPORTED ECOSYSTEM

The White House Report is significant for advertisers in that it acknowledges the benefits of the online-advertising-supported digital ecosystem. Consumers reap the "benefits of a robust digital ecosystem that offers a broad array of free content, products and services." The internet also permits small mom-and-pop shops to reach national and international audiences. The Report explains the "dizzying" number of players at work in this ecosystem, however, and argues that "[u]sers, more often than not, do not understand the degree to which they are a commodity in each level of this marketplace."

While the White House Report acknowledges that industry has worked hard to develop self-regulatory frameworks for online advertising that "provide consumers choice and transparency," it suggests that the system is not perfect, and that technologies have been slow to develop or are not used widely by consumers. For example, while the industry states that the "AdChoices" icon has been served in billions of ads, the Report argues that "only a tiny fraction of users utilize this feature or understand its meaning."

The Report expresses a particular concern about the "asymmetrical" relationship between individuals and the companies that collect information about them, because much of the data collection and analysis happens silently behind the scenes, so that consumers have diminishing control over the flow of their information. The Report also provides examples showing how algorithms used to analyze consumer data based on online and offline activity can offer personalized experiences that are beneficial to consumers, but expresses concern that "perfect personalization" could lead to both intentional and unintentional discrimination in pricing, services and opportunities.

Given the proliferation of data services companies that develop algorithms and provide alternative scoring—on everything from a consumer's ability to pay to whether he or she may be a social influencer—the Report makes clear that steps must be taken to prevent intentional and inadvertent discrimination or marginalization of vulnerable groups by the private sector. The Report does not suggest that self-regulatory frameworks should be abandoned, but rather that their current limitations should be acknowledged, explored and addressed as big data continues to evolve.

LIKELIHOOD OF PASSING NATIONAL DATA BREACH LEGISLATION

While it is not unusual for data breach legislation to be introduced each congress, the publicity surrounding the recent retail mega-breaches resulted in the introduction of five bills (four in the Senate, one in the House of Representatives) in the first five weeks of 2014. These bills, along with a June 2013 Senate bill, offer a variety of solutions to curb data breaches, including a national standard for data breach notification. Currently, the sponsorship and support for legislation rests primarily with the Democrats in the Senate. Democrats do not predict much movement in the House, as Republicans in both chambers have shown little appetite for legislation and are reticent to embrace the bills' provisions that call for the expansion of the FTC's authority. The outliers are two bipartisan bills: S. 1927, the Data Security Act, co-sponsored by Senators Tom Carper (D-DE) and Roy Blunt (R-MO), and S. 1193, the Data Security and Breach Notification Act, co-sponsored by Senators Pat Toomey (R-PA), John Thune (R-SD) and Angus King (I-ME). In February 2014, Representative Lee Terry (R-NE) publicly stated that he is working on data breach notification legislation, but it has yet to be introduced.

In conjunction with the data breach bills, there were five Senate hearings and one House hearing on this issue. The one point about which members—and hearing witnesses—agreed was the need for a federal, uniform data security breach notification standard. While it would appear that these statements show bipartisan support for national data breach legislation, the scope of the notification standard is not consistent in each bill. Determining a reasonable timeframe for notification, how to coordinate notification with law enforcement and prevent impeding investigations, and how to prioritize the level of harm from a data breach are all subparts of a national data breach notification standard that must be resolved in order to have enough support on both sides of the aisle.

Importantly, a number of the bills introduced to address data breaches include exceptions for health care providers, health plans and other entities covered by HIPAA. Should any of the

data breach bills begin to pick up steam, it will be important for HIPAA-regulated entities, as well as entities that fall outside of HIPAA but are nonetheless within the health and life sciences sectors, to assess how a bill's provisions may affect their use of individually identifiable health-related information.

Given the limited number of work days left in the mid-term election year legislative calendar, staffers from both parties do not believe there will be movement on this issue in the House. While the Democratically held Senate is in a better position to pass a bill, the competing bills would require member concessions and negotiations that are unlikely, although not impossible, before year's end.

AMENDMENTS TO THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

The ECPA of 1986 was written to protect electronic communications, including communications held in electronic storage. At the time the ECPA was enacted, lawmakers were unaware of how the internet and mobile technologies would change the landscape of electronic communications and storage (for example, the cloud). In March 2013, Chairman of the Senate Judiciary Committee Patrick Leahy (D-VT)—one of the original drafters of the ECPA—and Senator Mike Lee (R-UT) introduced S. 607, the Electronic Communications Privacy Act Amendments Act of 2013. The bill updates the ECPA, including the establishment of a search warrant requirement for the government to obtain the content of individuals' e-mails and other electronic communications that are stored with a third-party service provider. S. 607 was passed out of the Senate Judiciary Committee by unanimous vote on April 25, 2013.

On May 7, 2013, Representative Kevin Yoder (R-KS) introduced H.R. 1852, the Email Privacy Act. The House bill is a companion bill to S. 607. H.R. 1852 currently has 208 co-sponsors—135 Republicans and 73 Democrats. On the same day, Representative Matt Salmon (R-AZ) introduced another S. 607 companion bill: H.R. 1847, the Electronic Communications Privacy Act Amendments Act of 2013. H.R. 1847 has 24 co-sponsors—23 Republicans and one Democrat. Both bills were referred to the House Judiciary Committee's Subcommittee on Crime, Terrorism, Homeland Security and Investigations.

Amending the ECPA has broad bipartisan private sector support. In April 2013, a coalition of technology companies and associations, privacy groups and think tanks, including Google, Microsoft, the American Civil Liberties Union and Americans for Tax Reform, wrote to Judiciary Committee Chairman Leahy and Ranking Member Charles Grassley (R-IA), strongly urging members of the Senate Judiciary Committee to support S. 607.

Should one of the House ECPA amendment bills move forward, it will be important to evaluate its impact on HIPAA-regulated and non-HIPAA-regulated entities.

Where Do We Go from Here?

Given that these Reports were released simultaneously during Stanley Cup season, the famous Wayne Gretzky quote seems particularly apt: "skate to where the puck is going, not where it has been." That theme permeates the message of these two Reports. Big data has extraordinary potential to lead to yet unimagined benefits; the Reports challenge us to resist skating to where the puck has been, and instead figure out how to align "our legal, ethical, and social norms . . . to protect privacy and other values in a big data world"—the place where the puck undeniably is going.

So, how do companies do this?

First, both Reports endorse and emphasize the Consumer Privacy Bill of Rights, which was included in a 2012 White House Report entitled "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy." Click here for more information on the 2012 White House Report.

To recap, the Consumer Privacy Bill of Rights is founded on the Fair Information Practice Principles (FIPPs), and includes principles of:

- **Transparency**. Consumers have a right to easily understandable information about privacy and security practices.
- **Respect for Context**. Consumers have a right to expect that organizations will collect, use and disclose personal data in ways that are consistent with the

context in which consumers provide the data.

- **Security**. Consumers have a right to secure and responsible handling of personal data.
- **Access and Accuracy**. Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data are inaccurate.
- **Focused Collection**. Consumers have a right to reasonable limits on the personal data that companies collect and retain.
- **Accountability**. Consumers have a right to have personal data handled by companies with appropriate measures in place to ensure they adhere to the Consumer Privacy Bill of Rights.

Companies that participate in the big data ecosystem (those that facilitate, collect, process, analyze, use or benefit from "big data") should consider appointing an internal team to be responsible for the following items:

- Understanding the FIPPs and the Consumer Privacy Bill of Rights
- Analyzing how existing internal systems, policies, procedures and practices align with, or may need to be adjusted to reflect, these principles
- Evaluating how to ensure that new products and business models incorporate and reflect these principles, so they can stay ahead of where the potential regulation is headed

Second, companies should monitor the important concepts to watch described on page [TK], particularly those that are relevant for their industry and sector. A dedicated internal team can handle this, and also can be responsible for the following actions:

- Monitoring any further activity on these two Reports
- Assessing the impact on the business of any associated actions by industry, the White House, designated agencies or lawmakers
- Considering whether lobbying efforts may be appropriate to make the company's voice heard during what certainly will be the evolving discussion on this issue

Third, be creative. Given the Reports' caution about the potential limits on the "notice and consent" framework as a panacea for privacy controls in a big data environment, and in light of ongoing FTC consideration of how to protect consumer-generated digital information, software developers, engineers, app creators and other innovators in the digital economy should begin to think about tools that can be integrated into their products that provide greater control and flexibility downstream as new norms and expectations for privacy, transparency and accountability come into greater focus.

Both the White House and PCAST Reports acknowledge that there still is much more work to be done, many debates to be had and more stakeholder input to consider in the weeks and months ahead. There is no question, however, that with these two Reports, the White House has firmly declared big data the "new normal" and instructed businesses along with public policy and legal frameworks to adjust. The clear message: lace up your skates and make sure you head in that direction.

The material in this publication may not be reproduced, in whole or part without acknowledgement of its source and copyright. *The New Normal: Big Data Comes of Age* is intended to provide information of general interest in a summary manner and should not be construed as individual legal advice. Readers should consult with their McDermott Will & Emery lawyer or other professional counsel before acting on the information contained in this publication.

©2014 McDermott Will & Emery. The following legal entities are collectively referred to as "McDermott Will & Emery," "McDermott" or "the Firm": McDermott Will & Emery LLP, McDermott Will & Emery AARPI, McDermott Will & Emery Belgium LLP, McDermott Will & Emery Rechtsanwälte Steuerberater LLP, McDermott Will & Emery Studio Legale Associato and McDermott Will & Emery UK LLP. These entities coordinate their activities through service agreements. McDermott has a strategic alliance with MWE China Law Offices, a separate law firm. This communication may be considered attorney advertising. Previous results are not a guarantee of future outcome.

Office Locations

BOSTON
28 State Street
Boston, MA 02109
USA
Tel: +1 617 535 4000
Fax: +1 617 535 3800

BRUSSELS
Avenue des Nerviens 9-31
1040 Brussels
Belgium
Tel: +32 2 230 50 59
Fax: +32 2 230 57 13

CHICAGO
227 West Monroe Street
Chicago, IL 60606
USA
Tel: +1 312 372 2000
Fax: +1 312 984 7700

DÜSSELDORF
Stadttor 1
40219 Düsseldorf
Germany
Tel: +49 211 30211 0
Fax: +49 211 30211 555

FRANKFURT
Feldbergstraße 35
60323 Frankfurt a. M.
Germany
Tel: +49 69 951145 0
Fax: + 49 69 271599 633

HOUSTON
1000 Louisiana Street, Suite 3900
Houston, TX 77002
USA
Tel: +1 713 653 1700
Fax: +1 713 739 7592

LONDON
Heron Tower
110 Bishopsgate
London EC2N 4AY
United Kingdom
Tel: +44 20 7577 6900
Fax: +44 20 7577 6950

LOS ANGELES
2049 Century Park East, 38th Floor
Los Angeles, CA 90067
USA
Tel: +1 310 277 4110
Fax: +1 310 277 4730

MIAMI
333 Avenue of the Americas, Suite 4500
Miami, FL 33131
USA
Tel: +1 305 358 3500
Fax: +1 305 347 6500

MILAN
Via dei Bossi, 4/6
20121 Milan
Italy
Tel: +39 02 78627300
Fax: +39 02 78627333

MUNICH
Nymphenburger Str. 3
80335 Munich
Germany
Tel: +49 89 12712 0
Fax: +49 89 12712 111

NEW YORK
340 Madison Avenue
New York, NY 10173
USA
Tel: +1 212 547 5400
Fax: +1 212 547 5444

ORANGE COUNTY
4 Park Plaza, Suite 1700
Irvine, CA 92614
USA
Tel: +1 949 851 0633
Fax: +1 949 851 9348

PARIS
23 rue de l'Université
75007 Paris
France
Tel: +33 1 81 69 15 00
Fax: +33 1 81 69 15 15

ROME
Via A. Ristori, 38
00197 Rome
Italy
Tel: +39 06 462024 1
Fax: +39 06 489062 85

SEOUL
18F West Tower
Mirae Asset Center1
26, Eulji-ro 5-gil, Jung-gu
Seoul 100-210
Korea
Tel: +82 2 6030 3600
Fax: +82 2 6322 9886

SHANGHAI
MWE China Law Offices
Strategic alliance with
McDermott Will & Emery
28th Floor Jin Mao Building
88 Century Boulevard
Shanghai Pudong New Area
P.R.China 200121
Tel: +86 21 6105 0500
Fax: +86 21 6105 0501

SILICON VALLEY
275 Middlefield Road, Suite 100
Menlo Park, CA 94025
USA
Tel: +1 650 815 7400
Fax: +1 650 815 7401

WASHINGTON, D.C.
The McDermott Building
500 North Capitol Street, N.W.
Washington, D.C. 20001
USA
Tel: +1 202 756 8000
Fax: +1 202 756 8087

McDermott
Will & Emery

Boston Brussels Chicago
Düsseldorf Frankfurt Houston London
Los Angeles Miami Milan Munich
New York Orange County Paris Rome
Seoul Silicon Valley Washington, D.C.

Strategic alliance with MWE China Law Offices (Shanghai)

www.mwe.com