Bloomberg BNA

Privacy & Security Law Report®

VOL. 13, NO. 19 MAY 12, 2014

Big Data

Christin S. McMeley, Partner, Davis Wright Tremaine LLP

Views on Big Data Reports to the White House

On May 1 a big data policy report and an accompanying technical report on big data were presented to President Barack Obama. Among other things, the reports called for progress on national data breach notification legislation, Electronic Communications Privacy Act (ECPA) reform and the Obama administration's proposed consumer privacy bill of rights (13 PVLR 761, 5/5/14).

Bloomberg BNA Privacy & Security Law Report Senior Legal Editor Donald G. Aplin posed a series of questions to Christin S, McMeley, partner and co-chair of the Privacy and Security Practice at Davis Wright Tremaine LLP, in Washington. Before joining Davis Wright Tremaine, McMeley was vice president, chief privacy officer and deputy general counsel for Internet, telephone and cable company Charter Communications Inc. She provided her insights May 9.

 ISSN 1538-3423

BLOOMBERG BNA: Do you think the big data policy report to the president, and the accompanying technical report on big data, focused enough on the economic and other potential benefits of the analysis of large data sets in addition to debates over possible privacy intrusion dangers of big data?

McMeley: The policy report, ''Big Data: Seizing Opportunity, Protecting Values,'' goes farther to acknowledge the benefits that big data can provide than what we have seen in similar reports in the past, including the 2012 White House report that first promoted the Consumer Privacy Bill of Rights. Throughout the text of the policy report, the authors cite the beneficial uses in virtually every private and public sector and draw attention to the economic, social and personal advantages that big data can provide, yet warn of the risks and potential harms to civil liberties, consumers and personal privacy.

The accompanying technical report, authored by the President's Council of Advisors on Science and Technology (PCAST), also references some of the benefits of big data, but it is quick to point out that each benefit gained comes at a cost. In one section, the report's authors present a ''creepy'' scenario reminiscent of a Tom Cruise movie in which it is safe to leave personal items on the doorstep because there are cameras everywhere; every object is tracked through RFID chips; digital assistants offer us fashion advice and, no doubt, advertisements; airport security is no longer needed because identities are tracked; and erratic or dangerous behavior is predicted.

In the report authors' world, citizens act in the ''unconscious belief . . . that the cloud and its robotic servants are trustworthy in matters of personal privacy.'' Yet these same authors propose to take the ''burden of privacy protection'' out of the individual's hands and engineer privacy to conform to social norms. The problem with this solution is that privacy is itself contextual and, as the PCAST report points out, notions of privacy change generationally.

BLOOMBERG BNA: How do you react to the strong sense in the reports that the notice and consent model for data collection and use is difficult—or perhaps even impossible—and therefore largely irrelevant when considering privacy in the big data universe and say that perhaps a focus on how data are used would be more productive?

McMeley: It is true that in the connected world of today and tomorrow, adhering to the model of notice and choice will be difficult. While we may not have the best solution today, the foundational concepts of notice and choice should not be abandoned. Ontario Privacy Commissioner Ann Cavoukian may have stated it best when she said that accountability should be strengthened, but not at the expense of the Fair Information Practice Principles (FIPPs) or the role of the individual.

As the reports illustrate, consumers are overwhelmed with lengthy legal disclaimers that they do not understand, let alone read, and their bargaining power is often skewed, resulting in a take-it-or-leave-it scenario. The policy report acknowledges that the online advertising industry has been working for over a decade to provide consumers choice and transparency, yet the tools developed to provide consumers with privacy choices have not been widely used. The theories advanced as to why consumers don't affirmatively exercise their privacy choices range from obscurity or difficulty in use of the tools to ''privacy fatigue'' to the possibility that consumers may actually see a positive benefit to the trade–off—free content and ''discounts'' on goods or services in exchange for advertisements.

While we may not have the best solution today, the foundational concepts of notice and choice should not be abandoned.

The authors of the policy report are not giving up on notice and choice—yet. One recommendation offered by the policy report is for data brokers to follow the online advertising industry's lead and create a common website or online portal that would aggregate details about collected information and offer consumers better control over how their information is collected and used, perhaps similar to the portal that Acxiom recently beta tested. This may provide a partial solution to the problem, but based on the advertising industry's experience, it is not clear that consumers will even use this tool, nor will it solve every problem.

An alternative approach advanced by the PCAST report is for individuals to create a ''privacy profile'' that is offered and stored by third parties, such as app stores or browsers, who will then benevolently vet apps and services for the consumer to ensure compliance with the profile. When carried through to its logical end, if the services requested don't match the privacy profile, how does the take-it-or-leave-it option change? The additional suggestion ensuring privacy compliance by tagging every piece of data with permanent metadata to identify its origin only exacerbates the privacy problem and seems reminiscent of the ''creepy'' scenario posited earlier in the report.

Virtually every company would agree that one breach notification standard is better than separate state standards, and many would say that such a standard is worth defined and reasonable notification time lines with FTC oversight.

BLOOMBERG BNA: The report calls for a federal breach notice law to preempt the laws in 47 states and the District of Columbia with a single national standard, adding that it should be ''along the lines'' of the administration's May 2011 proposal, which called for a 60-day deadline for companies to notify individuals and a safe harbor for companies that informed the FTC they weren't notifying individuals because an investigation revealed there was ''no reasonable risk'' of harm to individuals (10 PVLR 730, 5/16/11). Is it time for a national breach notice standard, and would a law with the deadlines and risk of harm safe harbor envisioned by the administration four years ago be a good model?

McMeley: The practical reality is that companies have learned to live under the current regime, even though it can be difficult to apply the sometimes conflicting notice obligations when a breach affects customers in multiple states.

That said, virtually every company would agree that one breach notification standard is a better solution, and many would say that such a standard is worth defined and reasonable notification time lines with FTC oversight. Moreover, as we head into the next generations of breach statutes that bring in more data triggers and the possibility of shifting the costs of replacing credit and debit cards to the breached entity, a single standard is certainly an attractive alternative. But this only remains true if the federal breach notification standard preempts the state requirements and does not permit the states to enact legislation that provides higher perceived safeguards for each state's residents.

BLOOMBERG BNA: Does the big data policy report's call for Congress to move forward on the White House push for a consumer privacy bill of rights (11 PVLR 355, 2/27/12) effectively connect big data analytics to real-world consumer concerns about how their data are used? In other words, would a consumer privacy bill of rights as envisioned by the administration serve a meaningful data protection purpose in the context of big data?

McMeley: The Consumer Privacy Bill of Rights (CPBR) presents a framework that is flexible enough to address the issues of big data and create at least a meaningful dialogue toward modernizing outdated privacy laws that have not kept pace with technology. Whether this report will do more at the federal level than spawn government studies remains to be seen and appears unlikely in the current legislative environment. More probable is that the concepts in the CPBR will be used as guidance in ongoing self-regulatory initiatives, which serve to benefit consumers and individuals in the near-term.

If and when legislation is advanced, the PCAST report recommends establishing policies that address intended outcomes versus particular technological solutions. When we look to examples of such outcome-oriented legislation, we may turn to Section 5 of the FTC Act, which grants broad authority to the Federal Trade Commission to prevent entities from engaging in unfair or deceptive acts affecting commerce. The FTC has extended this broad grant of authority to the data security context and requires entities to maintain ''reasonable and appropriate'' data security standards. While such ''standards'' have faced criticism and even legal challenges (13 PVLR 621, 4/14/14), this is exactly the type of language we see when legislators and regulators desire flexibility. Unfortunately, they do not always provide the certainty the business community desires.

BLOOMBERG BNA: There is some focus in the reports of the big data implications for government surveillance, including the bulk collection of communications calling information and metadata, and a call for updating the Electronic Communications Privacy Act. Do you think the reports hit on the right points in this debate and may prove useful in continuing discussions about data collection for surveillance purposes?

McMeley: The report recommends updating ECPA to ensure the standard of protection for online, digital content is consistent with that afforded in the physical world. In other words, the government would have to get warrants to obtain the content of all e-mails, regardless of how old they are and whether they have been read, as well as the metadata associated with them. This is definitely a step in the right direction and eliminates what is no longer a usable distinction for e-mails or texts in transit or storage.

However, this recommendation does not address many of the National Security Agency activities that have come under scrutiny since the Edward Snowden leaks, such as the surveillance within some multiplayer online role-playing games or the collection of user contacts through secret arrangements with foreign telecommunications companies or allied intelligence services. Although the collection of ''upstream'' Internet traffic through the NSA's PRISM program was pursuant to warrants, when the program was revealed, many were surprised that individual warrants were not required, resulting in mass collection of personal information.

The recommendation that law enforcement's use of predictive data be subjected to careful policy review and that the public must be aware of the existence, operation and efficacy of such programs should serve to supplement the ECPA reforms and address some of these concerns.

BLOOMBERG BNA: Was there anything in the reports that surprised you, or perhaps more importantly you identified as something you would need to be prepared to discuss with your clients?

McMeley: At a high level, the idea of a flexible framework is generally appealing and recommendations that we shift to limitations on use versus collection make more sense, given the scale and automation of data col-

lection. But how those limitations are established will be where clients need to pay significant attention, as the report signals a move to take away at least some control from the individual. This is a fundamental shift from the current established regimes and it could significantly affect the way entities interact with their customers.

For instance, the policy report does not distinguish between first-party and third-party uses: it extends the obligations associated with operationalizing the Consumer Privacy Bill of Rights to all data holders, disregarding the privity of first parties to consumers. Currently, first parties may have certain statutory privacy requirements that can be modified by contract (i.e., the consumers' consent), but in any event, the first party is typically considered the owner of the data collected.

The position that data cannot be de-identified is problematic and can subject entities to significant liability for current business practices.

In the proposed new world, there would be a shift where certain rights are fundamental, similar to the European model. Consumers would own their data and harms of misuse would be defined, which sounds good, but it would also open the door to increased (and potentially more successful) privacy litigation.

Additionally, the erosion of de-identification, without any regard to proportionality of the efforts required to re-identify and the risks associated with the data in various contexts, presents a significant concern. We currently live in a world where consumer products and services require the sharing of certain information to function. Existing laws require data to be anonymous or de-identified prior to disclosure, such as in the case of medical information or video content. The position that data cannot be de-identified is problematic and can subject entities to significant liability for current business practices.

  PVLR ISSN 1538-3423