BIG DATA AND INSURANCE SYMPOSIUM

ATTORNEY GENERAL GEORGE JEPSEN
UNIVERSITY OF CONNECTICUT SCHOOL OF LAW
APRIL 3, 2014 (REVISED FOR PUBLICATION)

***

This Article reproduces the keynote address delivered by Connecticut Attorney General George Jepsen at the University of Connecticut School of Law's Spring 2014 Big Data and Insurance Symposium. In his address, Attorney General Jepsen describes the opportunities and challenges associated with the use of big data technologies. He stresses the need to consider personal privacy concerns at every step of the data collection and analysis processes. Moreover, he argues that self-policing is not enough and that it is vital for the government to play a role in defining and enforcing individual privacy protections. Attorney General Jepsen concludes by calling for regulators and industry to remember that they share the common goal of achieving an effective balance between protecting personal privacy and promoting the use of big data to create new business opportunities and more efficient service delivery.

***

I would like to thank the University of Connecticut School of Law, the Insurance Law Center, and the *Connecticut Insurance Law Journal* for hosting this important event and for inviting me to join the discussion here today.

We all know that big data has the power to change the world. In fact, it already has.

I like to imagine big data as the Colorado River in spring flood stage. It took a marvel of technology, the construction of the Hoover Dam – one of the largest man-made structures in the world when it was built in the 1930s – to contain that river and use its flow to generate electricity.

Harnessing big data – the torrents of information being generated every day – will take equivalent feats of technology. Engineers and data scientists are coming up with new ways to aggregate data and filter it to extract patterns and other information useful to consumers and business, such as the insurance industry.

But perhaps the biggest challenge is protecting the privacy of the men, women, and children whose personally identifiable information, patterns of behavior, preferences and buying habits, medical risks, and even their location can be filtered from the data stream.

As Attorney General, responsible for protecting the public interest of Connecticut and its citizens, I believe that this is an issue of paramount importance.

A White House working group voiced the same concern in May after a 90-day study of big data and its impact on the way we live and work.

Their report concluded that every sphere of life will be transformed by big data technologies. However, for society to enjoy the benefits of the knowledge they generate, personal privacy must be protected from the potential harm.

How data is collected raises one important privacy concern. How data is used and how it is protected are equally important questions. As the White House report noted, "volumes of data that were once unthinkably expensive to preserve are now easy and affordable to store on a chip the size of a grain of rice." The consequence of unlimited storage is that data, once created, is effectively permanent.

Another unfortunate corollary to the collection of data is that it can be lost or stolen, and it can be misused to illegally discriminate against individuals and groups. Loss of personal information – from Social Security and credit card numbers to medical and tax records – can result in the nightmare of identity theft. This crime is on the rise and the resulting legal and financial morass can take years and a great deal of money to correct, both for the victim and for the businesses and industries involved.

The Federal Trade Commission (FTC) reports that identity theft continues to top its national ranking of consumer complaints as it has for more than ten years. Last year, identity theft accounted for nearly 300,000 or 14 percent of all complaints to the FTC. Those numbers have continued to grow year after year. Connecticut is not immune to this frightening trend.

Soon after I took office in 2011, I created a multidisciplinary privacy task force chaired by Assistant Attorney General Matthew Fitzsimmons, who is one of the afternoon's panelists. The five attorneys who comprise the task force investigate data breaches that result in the loss of personally identifiable information of state residents, and seek appropriate remedies.

While my Office had responsibility to investigate data breaches, I worked with the Legislature to require that my Office be notified whenever a breach of security occurs involving the personal information of Connecticut residents. When that law took effect on October 1, 2012, the number of data breach reports nearly tripled overnight, underscoring the extent of the problem.

The notice requirement is triggered when unencrypted, computerized information is lost containing an individual's name and their Social Security, state identification or driver's license number, or bank account, credit or debit card number and any security code, access code, or password required for access to the account.

In the first year since the breach reporting law took effect, my Office received 427 reports of security breaches involving the personal information of nearly 588,000 Connecticut residents, more than sixteen percent of the state's population of nearly 3.6 million residents. Those are serious numbers.

What has been lost? Any and all information that can be collected: health records, tax data, student and faculty records, and credit card numbers by the thousands. The breaches can result from a sophisticated hacker invasion to something as simple as a lost laptop containing unencrypted data.

Breaches of security involving Social Security numbers are particularly serious. Because of the severity of the potential damage, we recommend that companies reporting such breaches offer two years of credit monitoring or identity theft protection service. Credit monitoring provides alerts to a consumer whenever an application for new credit is submitted to a credit-reporting agency. This early warning allows a consumer to take immediate action to dispute or even prevent a new account from being opened.

Connecticut is now one of forty-seven states with data breach notification laws, but I agree that a uniform federal approach through national data breach legislation would benefit business and better protect consumers.

While many companies do a good job at protecting sensitive data, others do not. The retail giants Target and Neiman Marcus reported massive data breaches last year that compromised the credit card numbers and other personal information of tens of millions of customers. The breach cost Target $61 million through the end of last year and will likely cost substantially more, as Target is facing more than eighty lawsuits and is under a number of government investigations. The National Association of Attorneys General (NAAG), for example, allows individual states to work on a bipartisan basis to resolve issues of nationwide concern. The NAAG multistate investigation into the Target and Neiman Marcus data breaches is being led by my Office, together with my counterpart in Illinois.

Target says "criminals forced their way" into its computer system, gaining access to guest credit and debit card information. Target said it has since closed the access point the hackers used, and the breach remains

under investigation. But this case, the Neiman Marcus case, and other high-profile security breaches show that hacker attacks are becoming more sophisticated. For business, government regulators, and law enforcement, it is becoming tougher all the time to stay ahead of the criminals. Data security is a global problem and the threat to privacy is real.

Harnessing big data poses an even greater threat to personal privacy from unauthorized collection, access, re-use, misuse, or loss of personal information. How do we address it? We must consider personal privacy concerns at every step of the data collection and analysis process.

The Internet industry, for example, favors self-regulation and agreements between individual companies, such as Google and Facebook, and their users to safeguard users' privacy. But that will not protect consumers when information about them is bought, traded, and sold by brokers or third parties that have no direct relationship to the consumer.

As we learned in the financial industry, self-policing is not enough. It is vital for government to play a role in defining and enforcing individual privacy protections as the Federal Trade Commission and the state Attorneys General currently do under the Health Insurance Portability and Accountability Act (HIPPA) and the Fair Credit Reporting Act (FCRA). The current legal framework focuses on obtaining user permission prior to collecting data and defines how that information will be used. The White House report suggests that a better approach may be to allow individuals to participate in the use and distribution of their information after it is collected.

Federal Trade Commission Chairwoman Edith Ramirez has asked Congress to give the FTC greater authority over data security. The changes she is seeking include: requiring companies, when appropriate, to notify consumers affected by a data breach; giving the commission authority to seek civil penalties to help deter unlawful conduct; and giving the commission jurisdiction over non-profit entities.

In 2012, President Obama proposed a national standard for protecting consumer data privacy where existing federal privacy rules do not apply. As proposed, the national Consumer Privacy Bill of Rights would pre-empt state laws inconsistent with the policy. However, the Federal Trade Commission and the state Attorneys General would continue to share authority to enforce the privacy rules as they now enforce HIPPA and the FCRA.

The Consumer Privacy Bill of Rights, for example, would give consumers: the right to control how personal data is used; the right to keep information being collected for one purpose from being used for an

unrelated purpose; the right to have information held securely; and the right to know who is accountable for the use or misuse of that information.

The White House study was part of the ongoing national discussion about big data. Your work will add to the debate. However, as we focus on the opportunities and challenges of big data, it is important to remember that regulators and industry are not working at cross-purposes. Effective use of big data has the power to transform our lives and create new opportunities for business, particularly the insurance, health care, and energy industries, through better cost controls and more efficient delivery of services.

Protections from misuse of their personal data will make consumers more willing to share their information, to engage in commerce, to participate in the political process and to seek needed health care.

As a result, we all have an economic and public interest in making sure an effective balance is achieved in protecting personal privacy with the generation of knowledge promised by the free flow and use of big data.

Thank you.