Bloomberg BNA

Privacy Law Watch™

Cybersecurity

Views on Personal Information, Cybersecurity Information Sharing Act From Jeewon Kim Serrato, Counsel, Debevoise & Plimpton LLP

The Cybersecurity Information Sharing Act (CISA)—incorporated as a part of the Consolidated Appropriations Act—requires businesses to scrub personal information not related to a cybersecurity threat from any threat indicator shared with the U.S. government under the act. CISA, however, doesn't provide a precise definition of what is personal information.

Bloomberg BNA Privacy & Data Security News Senior Legal Editor Daniel R. Stoller posed a series of questions to Jeewon Kim Serrato, counsel in Debevoise & Plimpton's Cybersecurity & Data Privacy Practice and former chief privacy officer of Fannie Mae, on what types of personal information should be protected and the affect of CISA across the corporate world.

 ISSN 0000-0000

BLOOMBERG BNA: CISA—including the interim policies and procedures—didn't directly define personal information. What do you think the definition should be and what types of personal information should be protected?

JEEWON KIM SERRATO: CISA defines ''cybersecurity threat,'' ''cyber threat indicator,'' ''defensive measure,'' ''security control,'' and ''security vulnerability'' but it doesn't define ''personal information.'' It does require, however, that the private company sharing information with the U.S. government remove any ''personal information or information that identifies a specific person not directly related to a cybersecurity threat'' from the cyber threat indicator.

To help identify categories of information that are considered sensitive and, therefore, protected by privacy laws, the joint DHS/DOJ document issued on Feb. 16, ''Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015'' (31 PRA, 2/17/16), highlights seven different types of information that may be potentially relevant:

- protected health information under the Health Insurance Portability and Accountability Act (HIPAA);
- human resource information;
- consumer information/history under the Fair Credit Reporting Act (FCRA);
- education history under the Family Educational Rights and Privacy Act;
- financial information under the Gramm-Leach-Bliley Act (GLBA);
- information about property ownership, governed by state laws; and
- information of children under the Children's Online Privacy Protection Act (COPPA).

There has been a lot of discussion and speculation on what ''should be'' included in the definition of personal information, should Congress ever tackle this question head on and actually deliver one unified definition, instead of the sectoral approach described above. It is one of the most difficult questions to answer and I'm glad the DHS and DOJ appear to be open to receiving industry feedback in the next coming months as they continue to develop the final guidelines that are due in June.

Until then, here are a couple of simple rules to help companies that are trying to do the right thing: (1) if some other law that applies to your business defines a category of data as personal information, you should treat it that way for CISA purposes; and (2) if you have your own existing policies and procedures that define ''personal information,'' you should follow those for CISA purposes.

Ultimately, the company is in the best position to determine the type of personal information data it uses, collects and stores, and treat that information in accordance with CISA, as well as other federal and state laws.

''Ultimately, the company is in the best position to determine the type of personal information data it uses, collects and stores, and treat that information in accordance with CISA, as well as other federal and state laws.''

BLOOMBERG BNA: Why was there a lack of this definition in the interim policies and procedures? Did this have to do with the CISA 60-day timeframe to provide the interim policies and procedures?

SERRATO: During the Feb. 24 event hosted by the Financial Services Roundtable, both speakers from DHS and DOJ made reference to the fact that the clock for the 60-day deadline to publish the interim guidelines started ticking on Dec. 18 when the law was passed, which meant the guidelines that required multiple agency coordination needed to be drafted and negotiated during the holiday season.

This isn't the first time, however, that federal agencies or Congress have attempted to grapple with this question. Even within federal agencies, agency-specific definitions of personal information or sensitive information are used and that the plurality of data classification schemes continue in the private sector where no uniform taxonomy exists in our current framework.

Although a specific definition would provide clarity to the industry, such a definition may also not account for the variety of business models, data collection efforts and industries captured under CISA's mandate. As DHS and DOJ develop their final guidelines, the industry has an opportunity to weigh in and help the federal government understand how data is collected, processed and managed in the private sector.

BLOOMBERG BNA: Does the European Union treat Internet protocol (IP) addresses different in terms of personal information than the U.S.? If so, why is there a difference?

SERRATO: In 2007, the Article 29 EU Working Party expressed the view that the definition of ''personal data'' in the Data Protection Directive was wide enough to encompass IP addresses. This question wasn't uniformly settled, however, and this question was referred to the Court of Justice of the European Union (''CJEU'') by German courts and heard in *Breyer* (Case C-582/14) Feb. 26. (37 PRA, 2/25/16). I wouldn't be surprised if the CJEU took the same view as the EU Article 29 Working Party and found that IP addresses can amount to personal data, despite the fact that they don't per se themselves identify an individual by name.

In the U.S., IP addresses are generally not considered to be personal information because the IP address is believed to attach to the device, not the person. The scenario of multiple persons living in the same house and using the same computer, for example, has been the dominant example used in the U.S. to argue that the IP address doesn't necessarily identify a person.

  PRA ISSN 0000-0000

The EU Article 29 Working Party, on the other hand, has said that server logs, IP addresses and web cookies fall within the definition of personal data in Article 2(a) of the Data Protection Directive if the individual to which they relate is identifiable, ***unless*** the ISP can distinguish with absolute certainty that the data correspond to users that can't be identified. The CJEU decision in Breyer will be closely watched in the EU and the U.S. and hopefully can provide clarity at least on how this issue will be treated in the EU.

"Teamwork is an important part of cyber preparedness and response, and this is true for the key stakeholders within the company, including the Chief Information Security Officer, General Counsel and the Board."

BLOOMBERG BNA: Cybersecurity threat information shared with international countries and other private sector entities aren't given liability protection under CISA. Should there be liability protection for cybersecurity threat information shared abroad and between companies and why do you think CISA doesn't cover this type of information sharing?

SERRATO: CISA doesn't contemplate any information sharing with non-U.S. authorities, and Congress or the U.S. federal government have no authority to grant liability protection to private companies from jurisdictions outside of the U.S. Thus, data sharing across countries raises significant jurisdictional issues, including whether it could subject companies to additional forms of liability or whether those countries have safeguards in place to store or use the type of information shared pursuant to CISA.

Although U.S. authorities can't grant liability protection, negotiations between U.S. and other foreign governments are ongoing to provide for such structure and framework within which private entities may be asked to cooperate with information sharing across borders. Very recently, for example, there have been negotiations between the U.S. and the U.K. to determine how companies may share personal information and other sensitive information in response to investigations. The negotiations have focused on the scope of information provided to U.K. law enforcement and the protections afforded to companies that share this information. It is likely that similar negotiations between the U.S. and other countries may be forthcoming.

BLOOMBERG BNA: Cybersecurity preparedness was referred to as a ''team sport'' by many of the Financial Services Roundtable panelists. How is cybersecurity a team sport not just between the government and companies but also within the interactions between a CISO and the board of directors or general counsel?

SERRATO: Teamwork is an important part of cyber preparedness and response, and this is true for the key stakeholders within the company, including the Chief Information Security Officer, General Counsel and the Board. Similar to how CISA must be implemented with DHS, DOJ, the Treasury and other agencies that have a stake in protecting this nation, several departments within a private company share the responsibility to play a part in protecting the company and its customers.

For example, deciding what needs to be scrubbed as personal information for CISA will require real teamwork between a company's legal and privacy team and its information security team – maybe more coordination than historically has been happening in threat sharing. The tech team's eyes and judgment will be needed to decide what threat information is important for DHS to receive. A lawyer's eyes and judgment—General Counsel, Chief Privacy Officer—will be needed to guide, if not make, the decisions about what needs scrubbing.

This is similarly the case when dealing with a data breach. You need the CISO's team to determine whether a breach happened and what data was exposed or taken. And you need the GC and maybe the CPO to oversee that investigation for privilege reasons; to determine if the state data breach consumer notification requirements are triggered; to be sure that the disclosures that go out are legally compliant; and to defend the litigations and investigations that typically follow a substantial breach. And overseeing all this coordination is the need for the Board to understand the risk posture of the company and for the senior management of the company to establish policies and procedures to document how this process will work.

As you can see, it takes effort across a company to address the various issues that arise in the cyber and privacy space. It is more than just how you interact with the government and the public—it is also how you instill a culture of cyber preparedness throughout the company as a whole.

"Consumers are beginning to understand the real-life impact of data breaches and expectations are changing in terms of how our data and privacy must be protected."

BLOOMBERG BNA: Lastly, how did you become interested and involved in privacy and cybersecurity law?

SERRATO: As my first job out of law school, I had the privilege of working on the Hill as legislative counsel while the PATRIOT Act was being reauthorized, the use of wireless surveillance and National Security Letters was being evaluated, and the question of balancing privacy and civil liberties with national security interests were debated in committee rooms and on the House floor.

The practice of privacy and cybersecurity law has evolved dramatically in the last decade with the rapid

changes we have seen from the industry and the increasing use of technology in our everyday lives. I was always interested in the intersection of technology, law and policy. Working in this area of law has provided me with opportunities to tackle cutting edge issues and explore how the modern society protects individuals, fosters innovation and connects societies.

Although we want more and more data to be used for good, whether it's for convenience, better decision-making or to fight the bad guys (as in the case of threat sharing under CISA), we don't want to do that at the expense of our privacy and civil liberties. Consumers are beginning to understand the real-life impact of data breaches and expectations are changing in terms of how our data and privacy must be protected. As privacy and cybersecurity issues become topics discussed in boardrooms and living rooms, the private sector and the U.S. government are also responding to make this a priority because I believe privacy and security aren't mutually exclusive and we all have a role to play in making sound data decisions.

  PRA ISSN 0000-0000