Draft Meeting Minutes
Subcommittee on Law, Policy, and Legislation
November 11, 2021
Virtual Meeting
1:00 pm – 2:00 pm

Member Attendance (7/10)
Senator Susan Lee and Blair Levin (co-chairs), Howard Feldman, Professor Michael Greenberger, Joseph Morales, Markus Rauschecker, and Paul Tiao.

Invited participants: Brian DeVallance and Curtis Dukes (Center for Internet Security) and Irene Ly (Commonsense.org)

Staff Attendance
Howard Barr (Assistant Attorney General & Principal Counsel, DoIT), Hannibal Kemerer (Director of Legislative Affairs, Office of the Attorney General), Michael Lore (Chief of Staff, Office of Senator Lee), and Dr. Greg von Lehmen (University of Maryland Global Campus, Assigned Staff to the Maryland Cybersecurity Council)

Meeting Summary

1. The chairs welcomed the members and guests. With a quorum confirmed, the minutes were called and unanimously approved without amendments.
2. The chair then turned to the agenda:
3. Discussion and approval of the minutes of the 01 June 2021 meeting
4. Discussion of possible bills for next session, e.g., some version of:
    a. The Ohio Data Protection Act (OADP)
    b. 2021 SB930 (Maryland Online Consumer Protection Act)
    c. 2021 SB 112/HB 148 (updates to MPIPA)
    d. 2020 SB 443/HB 888 (Security of Connected Devices)
    e. Other recommendations that the members may have
5. Other business of interest to the subcommittee
6. Adjourn

Ohio Data Protection Act

Senator Lee introduced two representatives from the Center for Internet Security: Brian DeVallance (Advisor to the Center) and Curtis Dukes (Executive Vice President & General Manager, Security Best Practices). She mentioned that she had attended the NCSL's September privacy summit and was interested in the OADP and similar laws because of their potential impact in incentivizing better security practices in the private sector.

Both Mr. DeVallance and Mr. Curtis thanked Senator Lee for the opportunity to provide information to the subcommittee. Mr. Curtis noted that the OADP enacted in in 2018. It was the first law in the Nation that aimed to incentivize businesses to implement a recognized cybersecurity framework or standard identified in the law (specific NIST special publications, CIS Controls, ISO 2700, or the FedRAMP security assessment framework). Similar laws have been passed in Utah and Connecticut, with Nevada and several other states likely to follow suit.

The incentives for implementation vary. The Ohio and Utah laws provide safe harbor against a suit in a state court or under state law in the case of a breach where the firm involved can demonstrate that it has made a reasonable effort to implement one of the cybersecurity frameworks or standards stipulated in the law. In lieu of safe harbor, the Connecticut law prevents punitive damages in such cases. The incentive could be something else, such as a tax credit or a state grant to implement a standard. Mr. DeVallance summarized by noting that short of regulation, offering the incentives for the private sector to enhance its cybersecurity is the best way forward.

Senator Lee asked if the specification of cybersecurity standards like ISO 2000 or CIS Controls creates a legal standard for the courts. Mr. DeVallance stated that it does not. But the laws provide that if a firm can prove that it implemented one of the approved standards, it earns the benefit.

Mr. Rauschecker asked two questions:

1) Whether there was any evidence about the rate of adoption by business under the Ohio law? Mr. Curtis answered that because the law is voluntary and the State does not track, the only evidence would come up in court cases. He underscored that the question is a good one and suggested that a survey might be done to address it.
2) How safe harbor provisions in the OADP changes the defense for a negligence claim? Mr. DeVallance answered that OADP and similar laws provide clarity about what a firm needs to do to claim safe harbor or other benefit. The difference is the specification of best practices or standards and demonstrating other things, like proportionality to scale of business, etc. Because of the specificity, it is easier to say whether there is negligence or not.

Maryland Online Consumer Protection Act (MOCPA)

There being no further questions, Senator Lee thanked Mr. Curtis and Mr. DeVallance and turned to a discussion of the MOCPA. Mr. Lore introduced Ms. Irene Ly from Commonsense.org to provide an update on the implementation of the California Consumer Privacy Act (CCPA). He noted that lessons learned in California could be helpful in shaping the MOCPA.

Mr. Ly observed that the focus of Commonsense.org is helping children use the internet safely. In this connection, she pointed out that:

- Children are vulnerable to privacy harms
- 98% of children under 8 have access to a mobile device, and their use is very surveilled
- Teenagers average eight hours a day accessing media
- Kids do not understand that the information they share is not private, and they give up more data than they might otherwise do.
- Kids don't distinguish well between advertising and fact

For these reasons, Ms. Ly stated that Commonsense.org supports the MOCPA. It will help protect the most vulnerable of the population.

Ms. Ly provided updates on the CCPA.

- She noted that the new California Attorney General has not published new rules but has gone out asking comments on a risk assessment, automated decision-making, what information should be provided to consumers so that they can easily exercise their rights over their data.
- The AG's office has enforced the law, notifying firms not in compliance.
- The AG's office has created a tool to help consumers draft notices of noncompliance to be sent to businesses. The AG has announced that such notice may trigger a 30-day cure period for firms not in compliance.
- The AG's office has released guidance that firms collecting data from consumer web activity must honor the Global Privacy Control (GPC) signal that the consumer has opted out of the sale of their personal data. Colorado is an example of another state that has included a similar provision in a recent data privacy law.

There was discussion around the private right of action (PRA) in the CCPA and similar laws in Colorado and Virginia. Mr. Feldman observed that PRA can be abused and that Attorney General offices tend to be more circumspect in enforcing the law. Mr. Rauschecker agreed that including PRA in CCPA-like laws is a major issue with pro and con sides. PRA does expand the bandwidth for enforcement, but on the other hand, it can be abused and is likely to trigger industry opposition. Mr. Lore suggested that providing for the opportunity to cure noncompliance ala the CCPA guidance could rescue PRA from these problems. Ms. Ly observed that in California, 75% of the firms notified as a result of PRA notification took advantage of the cure period to rectify their noncompliance.

Senator Lee commented that she would like to consider adding the GPC to the MOCPA. She commended Commonsense.org for its advocacy and thanked Ms. Ly for her presentation.

Updates to MPIPA

Senator Lee noted that in the last session there was extensive consultation with industry groups on the updates to MPIPA to reach a compromise. Genetic information was added to the definition of personal information. The timeline for notification was streamlined. Geolocation data had been taken out, but she suggested that perhaps it should be re-introduced.

Mr. Feldman raised the question whether there was an inadvertent flaw in the law. The current statute suggests that a breach that includes the unencrypted name of individuals linked to encrypted data defined in the statute would trigger a notification. He suggested that the intention of the statute is to trigger notification only when names combined with other unencrypted personal information in the law is exposed. Mr. Lore agreed with that assessment and indicated that he thought it would not be difficult to amend the definition.

In addition, Mr. Feldman stated that he thought the ten-day notification requirement under Section 14-3504(c)(2) and the seven-day notification under 14-3504(d)(2) are too short. He also questioned why under 14-3504(f)(3) in addition to the other notifications there also had to be notification by broadcast email.

Mr. Lore stated that the last point could be addressed. With regard to the ten-day notification, he suggested that the notification could be preliminary. Mr. Feldman noted that firms do not want to send notice unless they have confirmed as best they can that there has been an actual breach.

Security of Connected Devices

Senator Lee observed that the bill did not move last session. She expressed the need for more education about the bill. With more education, she thought the bill would fare better next session. There as no discussion of this agenda item.

Other business

Senator Lee mentioned that the General Assembly will start a special session on December 6. The Senate and House leadership have not announced how hearings will be conducted for the 2022 session, whether panels will testify by Zoom only or will be permitted to testify onsite again.

Adjournment

There being no further business and with no objections, Senator Lee and Mr. Levin adjourned the subcommittee at 2:15 pm.