Meeting Minutes
Subcommittee on Public Affairs and Outreach
Monday, March 17, 2025
10:00 am – 11:00 am
Virtual Meeting

Subcommittee Attendance (4/7)
Blair Levin (chair), Keith Moulsdale, Joe Morales, and Markus Rauschecker

Others Present
Howard Barr (Assistant Attorney General and Principal Counsel, DoIT, and Council chair designate) and Dr. Greg von Lehmen (University of Maryland Global Campus, staff to the Council)

Meeting Summary

1. The chair welcomed the members, confirmed the quorum, and noted the posting of the May 10, 2024, meeting of the subcommittee
2. He then opened the floor for a discussion of policy issues that the subcommittee might agree to explore with a view to making recommendations for the State. In this connection, Mr. Rauschecker, speaking for the Center for Health and Homeland Security (CHHS), noted that the Center might be able to provide interns from the law school to conduct research in support of that agenda. Regarding policy issues:
    a. AI. Mr. Moulsdale proposed looking at AI-related policy issues. He noted that Maryland has enacted a legislation on AI applications in State government and that there were number of AI-related bills in play during the current legislative session. But there are likely important issues the State has not yet addressed. As a starting point to identify gaps, he suggested comparing policies that Maryland has implemented to date what other states—California, Colorado, and perhaps others—have done as a basis for policy recommendations.
    b. Domain name registration. Mr. Moulsdale observed that the ease of registering domain names facilitates phishing, a leading cause of cybersecurity breaches. He suggested considering whether there should be a red flag law as exists in the financial sector. Mr. Morales said another analogy is the trademark law requirement that new trademarks not cause confusion with existing ones in the market. Mr. Moulsdale thought it might be useful for the subcommittee to get a primer on how the domain name system works. The related research project could summarize the policy issue and examine analogies in other areas of law that might be informative of a policy to regulate domain name registration.
    c. Access to PII of Maryland residents by DOGE. Mr. Levin noted that the Council is a nonpartisan body. He observed that DOGE's wide access to the PII of citizens

is raising questions among federal privacy law experts. As Maryland residents are caught up in DOGE's activities, he suggested that the subcommittee research the issue, consider what appropriate avenues of State action might be available to challenge this, and make an appropriate recommendation.

d. Personal liability standards for boards of directors in breach cases. Since cybersecurity starts with governance, Dr. von Lehmen asked whether the subcommittee would be interested in examining the question of personal liability for board of director members for breaches. This would come into play where it could be shown that a contributing factor was the lack of a reasonable cybersecurity program.

   Mr. Rauschecker noted that private right of action would be problematic for industry and difficult to achieve legislatively. Mr. Moulsdale suggested that more likely to succeed would be the idea of investing the power to pursue such actions in the Attorney General's Office. Nonethless, he stated that the bar should be fairly high and that a number of questions would have to be answered, such as what evidence would a company have to show in order to demonstrate it had a 'reasonable' cybersecurity program?

   As an alternative to affecting the risk/investment calculations of boards, Mr. Moulsdale asked whether a cybersecurity safe harbor law might achieve the same goal. He pointed out that Ohio has long had such a law and that a number of other states have followed. Dr. von Lehmen noted that the Center for Internet Security has a model statute that has a defined reasonableness standard that has in fact informed these state laws. Mr. Rauschecker observed that it would be important to see what the experience had been in the application of those laws in Ohio and elsewhere. Questions include how often the safe harbor law has been invoked? How difficult was it for companies to claim it? What difficulties have courts has in applying the 'reasonableness' standard?

   In summing up, research questions concerned: 1) if any, what standards for board of director personal liability exist in federal and/or state law, what is the standard, and analogously, what might a standard look like for the duty to ensure reasonable cybersecurity? and 2) how has CIS addressed the question of what constitutes a "reasonable" cybersecurity program and what has been the track record of cybersecurity safe harbor laws in other states?

   Following the discussion, the subcommittee moved to vote on the suggestions. Mr. Moulsdale endorsed the list of policy issues and related research questions and apologized for having to leave the meeting. Messers Levin, Morales, and Rauschecker also endorsed the list and questions.

Some of the members expressed a willingness to consult directly with the interns on their suggestions. As action items, Dr. von Lehmen indicated that he would follow up with Mr. Rauschecker on the timing and availability of CHHS interns and would organize the next subcommittee meeting for a brief by CIS on its model safe harbor statute.

With no further business, the meeting was adjourned at 11:15 am.