Draft Meeting Minutes
Maryland Cybersecurity Council
Subcommittee on Law, Policy, and Legislation
Wednesday, October 03, 2018
10:00 am – 12:00 pm
College Park Marriott at UMUC
Room 3114
3501 University Boulevard East
Hyattsville, Maryland

Attendance

Subcommittee members attending: Senator Susan Lee, Blair Levin, Patrice Drago (Chief of Staff for Delegate Ned Carey), Howard Feldman, Joseph Morales, Jonathan Prutow, Markus Rauschecker (for Professor Michael Greenberger), and Paul Tiao. (Quorum present 8/9)

Staff: Howard Barr (Assistant Attorney General and General Counsel, DoIT), Michael Lore (Chief of Staff, Office of Senator Lee), and Dr. Greg von Lehmen (Staff, Maryland Cybersecurity Council).

Members of the public: Kevin Callahan (CompTia), Ariel Fox Johnson (Commonsense.org), Shum Preston (Commonsense.org), Katie McGinnis (Consumer Reports), Salena Musuta (Mozilla Fellow at Consumer Reports), and Carl Szabo (NetChoice).

Meeting Summary

1. Welcome by Senator Lee who announced that a quorum of the subcommittee was present. She provided an opportunity for representatives of organizations who came to the meeting to introduce themselves.
2. Call for the minutes of the June 5, 2018, meeting of the subcommittee. The minutes were approved by the members.
3. Discussion of new business:

a) California Consumer Protection Act (SB 1121). Ms. Ariel Fox Johnson (Commonsense.org) briefed the subcommittee on the most current version of the statute. Questions and discussion followed.

b) Safe harbor. This discussion focused on Ohio 2017 SB 220 as a possible model for Maryland. Howard Feldman noted that safe harbor offering an affirmative defense in the case of a breach will not deter plaintiff's attorney from suit to obtain a settlement. Better would be a presumption that a standard of care had been met in the case of firms that implement a recognized cybersecurity standard. Paul Tiao drew the subcommittee's attention to the federal SAFETY Act as a potential model for encouraging businesses to implement a recognized security standard. The act provides certain liability protections for entities that have received a designation or certification from the Department of Homeland Security for the sale or provision of "qualified anti-terrorism technology" to customers.

c) Ransomware. Michael Lore explained the work with the legislative committee on this issue. He drew attention to a Michigan statute on the subject and also a compilation of ransomware attacks on state and local government entities and whether ransom was paid.

d) Net neutrality. Articles in the media have commented on the cybersecurity implications of net neutrality. Mr. Levin drew attention of the subcommittee to the recent DoJ suit filed against California in which the Department argues that net neutrality issue has been preempted by federal action. A concern is that the Court could hand down a decision that is too broad and could wipe away state laws on cybersecurity issues. His recommendation is that Maryland should weigh into

the legal action on the side of California in order to protect the progress that states have made in the area of cybersecurity.

e) Internet of Things (IoT). The subcommittee discussed California's SB 327. The law requires manufacturers to take reasonable steps to secure IoT devices defined as those that have IP addresses and communicate via Bluetooth. These steps include unique default passwords and offering consumers the option of changing passwords.

f) Algorithms used to determine credit and consumer access to other services. Michael Lore distributed an article and briefed the subcommittee on the issue.

4. Given the subcommittee's interest in the foregoing, Senator Lee will brief out the discussion of the subcommittee for the consideration of the full Council at its October 16 meeting.

5. The meeting was adjourned at 11:20 pm.

Subcommittee Briefing

CCPA

My name is Ariel Fox Johnson, Senior Counsel with Common Sense Media. Common Sense was a sponsor of California's precedent-setting consumer privacy law, the California Consumer Privacy Act (CCPA).

Common Sense--which is celebrating its 15th anniversary this fall--is dedicated to helping kids and families thrive in a world of 24/7 media and technology. More and more, that means ensuring children and families' privacy as they interact with a host of devices and corporate interests eager to collect, sell, and share their information, often in ways individuals do not expect or understand.

Kids Are Uniquely Vulnerable

It's not hyperbole to say that children today face surveillance unlike any other generation -- their every movement online and off can be tracked by potentially dozens of different companies and organizations. We know that ninety-eight percent of children under 8 in America have access to a mobile device at home.[1] Half of teens say they feel addicted to their mobile devices,[2] and those teens overall consume an average of nine hours a day of media.[3] Young people will spend their entire lives connected in order to get an education and participate in modern society. They are more likely to connect via mobile devices that gather information constantly. Furthermore, kids are prone to sharing and impulsive behavior, more susceptible to advertising, and less able to understand what may happen to their personal information.

Our kids are uniquely vulnerable to privacy harms. And growing lack of privacy and distrust of the online world impacts every family, and could significantly impact the personal development of young people. At Common Sense, we believe kids need the freedom to make mistakes, try new things, and find their voices without the looming threat of a permanent digital record that could be used against them. They deserve a world in which their daily musings to friends are not assessed by corporations looking to turn a profit or by nefarious actors looking to manipulate their behavior.

It is our goal to help our tens of millions of American members improve the digital wellbeing of their families--and while in many instances that means teaching parents, teachers, and kids good digital hygiene practices and skills, it also means ensuring there are baseline protections in place. Even extremely savvy digital citizens are powerless if they do not know what companies are doing with their information, if they cannot access, delete, or move their information, or if they

---

[1] The Common Sense census: Media use by kids age zero to eight (2017), available at https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-kids-age-zero-to-eight-2017 [2] Common Sense: Technology Addiction: Concern, Controversy, and Finding Balance (2016), available at https://www.commonsensemedia.org/research/technology-addiction-concern-controversy-and-finding-balance.

[3] The Common Sense Census: Media use by teens and tweens (2015), available at https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-tweens-and-teens.

have no choices with respect to the use and disclosure of their information. And an individual has no ability to prevent a corporate or government data breach.

Privacy Principles and the CCPA

Recently we asked parents across the country how they want to protect their privacy rights, and what tools would help their families. These views informed the values--including consent, transparency, and control--that guided our approach in California.

For example:

- More than nine in 10 parents and teens think it's important that sites clearly label what data they collect and how it will be used.[4]
- 69 percent of teens and 77 percent of parents say it is "extremely important" for sites to ask permission before selling or sharing their personal information.
- Only a third of teenagers and a quarter of parents agree that social networking sites and apps do a good job of explaining what they do with users' data.
- And 82 percent of parents and 68 percent of teens are at least "moderately" worried that social networking sites use their data to allow advertisers to target them with ads.

In other words, the American people are very clear about privacy: they feel vulnerable online today and want much stronger and more comprehensive privacy protections.

The CCPA is a first step towards giving them those protections. It is the first generally applicable consumer privacy law in America--not limited to financial or health information, or any specific entity, but recognizing that Americans have privacy rights in all of their information, no matter who holds it. This information is being collected, used, and shared in unprecedented and unexpected ways.

In California, the statewide ballot initiative process drove the legislation. A privacy initiative focused on notice and saying no to sales of data was the catalyst that led to larger discussions to develop more comprehensive privacy legislation. At Common Sense, we worked hard to expand substantive rights under the law--including opt-in rights (which we achieved for minors under 16), and new access, deletion, and portability rights. The California Consumer Privacy Act ultimately passed unanimously through both houses of the California legislature.

---

[4] *See* Common Sense and Survey Monkey Poll (2018), available at

https://www.commonsensemedia.org/about-us/news/press-releases/common-sense-and-surveymonkey-poll-finds-pri vacy-matters-for-parents.

The law goes into effect in 2020 and will allow California residents to access the personal information companies collect about them-- and port their data to another platform, or demand the deletion of their data (with exceptions) if they wish. Californians can tell companies to stop selling their personal information. And kids under 16 or their parents must opt in before their data is ever sold. The Attorney General primarily enforces violations of the law--with a private right of action for certain data breaches--and the law applies equally to service providers, edge companies, and brick and mortar entities.

CCPA and Maryland

In the CCPA, personal information is defined very broadly, to include any information that "identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." This includes device and unique identifiers. The type of information protected under the data breach provisions, and which can give rise to a private right of action, is more narrow -- SSN, drivers license, credit or debit account and password, medical, or health information.

When you think about what information is protected under current Maryland law, it is more similar to the type of information protected under California's data breach provisions--as I understand it, MPIPA protects information like: SSN, driver's license, and financial account information.

As you consider a privacy law to protect Marylanders, we understand MPIPA will be a starting point. We urge you to think broadly about the best way to protect families and citizens today. The CCPA is a good first step, but consumer privacy protections could be stronger. We and other consumer groups are interested in seeing inclusion of minimization of data collection and use and ensuring that discriminatory financial practices are sufficiently prohibited. We would also like to see an expanded private right of action, and extend reasonable security standards for all information. (Though California did just sign into law an internet of things bill requiring reasonable security on connected devices.) Maryland can layer on additional protections, while keeping the baseline protections consistent with California's.

Next Steps in California and Across the Country

We look forward to working with Maryland on a strong consumer privacy law. As we look ahead, I wanted to update on developments in California and elsewhere: Industry is working hard to weaken the California law -- or preempt it entirely at the federal level. They particularly don't like the private right of action. They'd prefer a more limited definition of personal information. They don't want to have to provide access to your information--even though this is

offered to Europeans. We do not believe the federal government will pass a privacy law this year. (There are 50 data breach laws and still no federal one.) We also do not believe that the California legislature will now take away the new consumer protections it has provided.
Nonetheless we are remaining vigilant.

We are also working to ensure that the AG has sufficient resources. We supported a 700k funding bill recently signed into law. And we will engage in the rulemaking process that the AG must undertake.

We are also working to expand these rights to others across the country--like here in Maryland. The right to privacy is a fundamental American right, but one that is all too often violated online and overlooked by our elected officials. Families from every state in America are standing up to demand better privacy rights now--and Maryland can play an important role in winning that for all of us.