Statement of Aleecia M. McDonald, PhD
Assistant Professor of the Practice, Information Networking Institute,
Carnegie Mellon University
Member of the Board of Directors, Privacy Rights Clearinghouse

California Assembly Committee on Privacy and Consumer Protection

The California Consumer Privacy Act of 2018

27 June, 2018

Mister Chair, Senators, and members of the committee, thank you for the opportunity to speak about Californian’s privacy today.

I am Aleecia M. McDonald, and I start next week as an Assistant Professor at Carnegie Mellon, based at our Silicon Valley campus. I am also here as a member of the board of directors for the Privacy Rights Clearinghouse. When I last appeared before you, I was the Director of Privacy at the Stanford Center for Internet & Society, where I remain affiliated as a non-resident fellow. Prior to Stanford, I worked for Mozilla as a senior privacy researcher and co-chaired the efforts to standardize the Do Not Track web browser option within the World Wide Web Consortium (W3C.) The work on Do Not Track has parallels and lessons for our current legislative efforts, as I will touch upon further.

I. Development of Privacy Rights

But first, as academics do, let me take a spend minute on history. The California Constitution includes the right to privacy in Article I, Section 1. On the Federal level, guidelines for Fair Information Practice Principles (FIPPs) developed in the 1970s in response to concerns about databases held on mainframes.\(^1\) These principles are known as *Notice, Choice, Access, Security,* and *Enforcement,* and have been adopted by the Federal Trade Commission (FTC,) the Federal Communications Commission (FCC,) the Department of Homeland Security (DHS,) the White House’s

---

Online Consumer Bill of Rights, and form the basis of much privacy thinking and law in Europe. Yet these basic principles of the past forty-five years remain mostly aspirational. The California Consumer Privacy Act will help to realize the Fair Information Practice Principles.

Technology moves quickly while law is slow. Policy makers are prudently reluctant to risk innovation and fear unintended consequences. The FTC pursued an “industry self-regulation” approach. For instance, the FTC encouraged companies to post privacy policies. In 1998, the FTC commissioned a report that found while 92% of websites collected data, only 14% provided notice of their practices. Most companies simply ignored the FTC’s call for privacy policies. California took action and passed the California Online Privacy Protection Act (CalOPPA,) making California the first state to require privacy policies in 2004. From there, privacy policies became the national norm.

Beyond privacy policies for Notice, the FTC encouraged industry to build tools to empower citizens and to obtain the full set of Fair Information Practice Principles. During my work co-chairing Do Not Track, over 100 policy makers, advocates, industry leaders, and researchers within the US and globally spent years on seemingly small details. We worked out the finer points of how to build an opt-out system that allows for privacy yet can be implemented in the real world. This bill encompasses the lessons learned from Do Not Track.

Privacy is not something an individual company can solve. When I worked for Mozilla, we wanted to run an ad campaign for the Firefox web browser. Mozilla could not find any ad brokers offering ad placement without tracking. Not one.

---

There is an interlocking set of companies that transfer data that identify specific users. This is by no means an intractable problem, but it is one that takes coordination. Worse, currently no company has the incentive to go first. The bill before you today cuts through the twin problems of coordination and incentives in a way that industry self-regulation, standards bodies, and software tools simply cannot.

II. Support for the California Consumer Privacy Act of 2018

History addressed, now I would like to discuss supporting the California Consumer Privacy Act. When I read the text of the related proposition, I was struck by how carefully crafted it was, and how it takes a reasonable and feasible next step forward on consumer privacy protections. Within the Privacy Rights Clearinghouse we had a challenge: we have never endorsed propositions. We have concerns about how difficult it is to make updates to propositions, and with technology moving so quickly, the one thing we know is change abounds. In the end, we endorsed anyway, because the protections offered by the proposition are so overdue. We are even more comfortable with a bill.

In particular, our endorsement\(^4\) is based upon California citizens gaining:

- The right to know what information a business has collected about them.
- The right to request that information collected about them be deleted or provided in a way that will allow them to transport the data in a usable format to another service or business.
- The right to know when their personal information has been sold to third parties, to know what categories of third parties their data was sent to, and to opt out of any sale of their information to third parties.

\(^4\) Please see Privacy Rights Clearinghouse’s memo to Senator Hertzberg and Assemblymember Chau, “RE: Support AB 375 as amended (Hertzberg and Chau),” June 26, 2018, by Emory Roane.
• The right of Californians to not be discriminated against in service or price for choosing to exercise their privacy rights.

• A limited private right of action in the event of a data breach.

• The creation of funding mechanisms to encourage robust Attorney General enforcement of these rights.

There were aspects of the proposition that we preferred, but overall, we are happy with the long-term prospect of legislation. As a result, Privacy Rights Clearinghouse endorsed the California Consumer Privacy Act. We look forward to working with policy makers and the Attorney General’s office to ensure the law fully protects Californians.

To conclude, the law before you today is based upon 45 years of privacy rights work. It does not solve all privacy issues. It is, however, a very good next step as we work to empower citizens and protect democracy itself from out-of-control data collection.