Testimony on Alaska SB 118

Matthew Erickson
Digital Privacy Alliance

April 3, 2018

Chairperson, members of the committee, thank you for the opportunity to testify on SB 118, the "Right to Know Act". I am the executive director of the Digital Privacy Alliance, a nonprofit made up of tech companies, technologists, attorneys, academics, and common citizens that recognize a need for better consumer privacy online. I am also the Director of Client Services and Technology for SpiderOak, a technology company dedicated to online privacy and security. This bill is essential in guarding Alaskan citizens' privacy and seeks to give Alaskans the information they need to be able to make informed market choices about with whom they share their personal data with by ensuring that once every twelve months Alaskans can request a report from online services as to what data of theirs was shared with whom. I am particularly glad to be testifying in Alaska, as Alaska has shown itself as a leader in protecting personal information rights. I'd like to start by discussing the problems that we need to overcome.

Today's world all but requires people to be interacting through the Internet to accomplish everyday tasks, from banking and healthcare, to purchasing goods and services, and to connecting with friends and family. My attendance here providing testimony is based on outreach made over the Internet. This greatly empowers people all over the globe, especially those formerly isolated, making commerce stretch farther and the world seem smaller. Unfortunately, much of our activity in this new everyday life is recorded, collected, and sold to unknown places for unknown purposes. This unregulated data collection has stark consequences in light of not just the increasingly-common data breaches, but the revelations of the collaboration between Facebook and Cambridge Analytica. It is important that

we as a society empower everyday people to know what is going on with the data that represents who they are.

In today's age, corporations are collecting data on people all across the Internet via a wide variety of means to monetize that data and better market to those people. In a broad view, that's not the problem. Marketing-based systems have created a means to monetize increasingly better online tools that have enabled more and more people to be able to afford higher quality tools to communicate around the world. Unfortunately, that data is often abused, breached, or otherwise misused in ways that go far beyond funding development of a platform. Facebook, Twitter, and Instagram provided warrantless live streams of protest data to law enforcement through a company called Geofeedia in 2016[1]. Regular massive data breaches illustrate just what dangers we face from the large centralized collection of personal information. Alaskans suffer through having their personal information revealed by organizations they may have no knowledge of even interacting with.

Normally, we would first hope that if a company is a bad actor, people would cease doing business with it and it will naturally either correct its actions or go out of business. This is why we put value in organizations such as the Better Business Bureau. However, we lack the information to make such choices in the online space. Organizations such as Facebook will commonly track users not just outside of the Facebook website, but also people who have chosen to not have a Facebook account to begin with[2]. How are we, as individuals, supposed to make decisions on who gets the business of our personal data online without appropriate knowledge to support these decisions? No other industry gets to effectively charge you what they want for service and hide the invoice. And unlike other forms of payment, your personal information can't be gotten back once it's shared.

Arguments against providing these invoices to customers typically take the form that they are undue burdens on businesses. However, businesses will be able to comply easily with a minimum of overhead. Generally speaking, there are two broad categories of how organizations collect and sell data: either they handle it simply, where all user data in given categories is collected and set to a set number of advertising partners, or they have more complicated schemes. In the first case, a form letter is generally all that will be necessary. At the simplest end, an auto-responder can issue reports on demand. More complex uses of user data will be

[1]https://www.theguardian.com/technology/2016/oct/11/aclu-geofeedia-facebook-twitter-instagram-black-lives-matter

[2]https://spideroak.com/articles/facebook-shadow-profiles-a-profile-of-you-that-you-never-created/

necessarily accounted for already within company databases. When a company is built on monetizing user data in this manner, it will have an understanding of what was sold to whom and for how much, this being a necessity to properly provide fiscal accounting for the business. Reports can then be generated for users under the terms of this bill out of this same data. Additionally, larger multinational companies, or any company wishing to extend overseas, already has to comply with similar regulations in the EU and Canada, making compliance a simple matter of enabling the same functionality for Alaskans.

Finally, many organizations are now seeing trends towards growing distrust in the online economy. A recent Guardian headline asked if 2018 was the "year of the neo-Luddite?"[3]. Small startups labor most not under regulatory burden, but the problems of trying grow revenue. A growing distrust of online services only serves to slow down business. If the legislature wishes to help small businesses grow, the best thing it can do is help level the playing field for consumers to regain that trust.

Technological innovation is incredibly useful and beneficial to society. It saves time and money, and can also save lives. Analytics-driven service monetization also makes the cost of many advanced services down to what people have to spend-which for poorer citizens, is their personal information. It's not complicated for business to make sure citizens are empowered to choose with whom they share their personal data, and in return they can reverse the trend of increasing distrust in participating in the online economy. This bill will help make sure that the citizens of Alaska can have that trust. Thank you.

[3]https://www.theguardian.com/technology/2018/mar/04/will-2018-be-the-year-of-the-neo-luddite