**GENERAL COMMITTEE MEETING**

Thursday, July 18, 2019

3:00 PM to 4:00 PM

Healthcare Leadership Council

750 9th Street, NW, Suite 500 Washington, D.C. 20001

**Conference Line:** 857-232-0157, **Code:** 30-40-73

1. Welcome and Introductions
2. Legislative Update
3. Beyond HIPAA
    a. Protecting Personal Health Data Act **Attachment 1**
4. National Patient Identifier
5. McCarthy Op-ed **Attachment 2**

# Klobuchar, Murkowski Introduce Legislation to Protect Consumers' Private Health Data

June 14, 2019

***Legislation focuses on data collected from health tracking devices and apps as well as DNA testing kits***

WASHINGTON – U.S. Senator Amy Klobuchar (D-MN) and Senator Lisa Murkowski (R-AK) introduced new legislation today to protect consumers' private health data. While recent reports have highlighted how home DNA testing kits and health data tracking apps have given companies access to unprecedented levels of consumer health data, current law does not adequately address the emerging privacy concerns presented by these new technologies. The *Protecting Personal Health Data Act* addresses these health privacy concerns by requiring the Secretary of Health and Human Services to promulgate regulations for new health technologies such as health apps, wearable devices like Fitbits, and direct-to-consumer genetic testing kits that are not regulated by existing laws.

**"New technologies have made it easier for people to monitor their own health, but health tracking apps and home DNA testing kits have also given companies access to personal, private data with limited oversight,"** Klobuchar said. **"This legislation will protect consumers' personal health data by requiring that regulations be issued by the federal agencies that have the expertise to keep up with advances in technology."**

**"I continue to hear from Alaskans about privacy concerns when it comes to individual data. Protection of personal information, and health information in particular, is an important issue to me and to the people in our state. That's why I have pushed for data privacy protections for all consumers, and am proud to cosponsor this bipartisan legislation addressing health data privacy and security. Information about an individual's health is incredibly personal and keeping this information private and secure must be a priority,"** Murkowski said.**"This legislation takes important steps to ensure guidelines are created for security and privacy protections of modern health information. Our policies must evolve to keep up with advancements in recent technology. By enacting important modern protections for consumers' personal health data, our bill puts the privacy of American consumers first."**

The *Washington Post* recently reported that a pregnancy tracking app has been selling user data to employers, and another report revealed that health apps for users battling depression or trying to quit smoking are selling personal details they collect to third parties, like Google or Facebook, without user consent. A subsequent poll ashowed that users of these apps cared about privacy, but they also thought the digital trackers were too valuable to give up. Current laws such as the Health Insurance Portability and

Accountability Act of 1996 were enacted by Congress when many of the wearable devices, apps, social media sites, and DNA testing companies collecting and sharing health data today did not exist. As science continues to drive technological innovation, we must not sacrifice privacy.

The *Protecting Personal Health Data Act* would:

- Require the promulgation of regulations to help strengthen privacy and security protections for consumers' personal health data.
- Ensure that these regulations take into account:
    - Appropriate standards for consent that account for differences in sensitivity between genetic data, biometric data, and general personal health data, and that complement existing regulations and guidance; and
    - The ability of consumers to navigate their heath data privacy options, and to access, amend, and delete a copy of the personal health data that companies collect or use.
- Create a National Task Force on Health Data Protection that would evaluate and provide input to address cybersecurity risks and privacy concerns associated with consumer products that handle personal health data, and the development of security standards for consumer devices, services, applications, and software. The Task Force would also study the long-term effectiveness of de-identification methodologies for genetic and biometric data, and advise on the creation of resources to educate consumers about direct-to-consumer genetic testing.

The bill is endorsed by Consumer Reports.

"Consumer Reports supports the Protecting Personal Health Data Act because the current legal framework for privacy around health data is out of date and incomplete. Protecting the legal right to privacy for users of new health technology is about ensuring consumers have the freedom to take advantage of promising new health technology without losing the right to privacy or facing harm such as discrimination," **said Dena Mendelsohn, Senior Policy Counsel for Consumer Reports.**

Klobuchar has fought to lower prescription drug prices, invest in research, and protect coverage for people with preexisting conditions. She has also been a leader in the fight to protect consumers' private information. Klobuchar and Senator John Kennedy (R-LA) introduced the *Social Media Privacy and Consumer Rights Act,* legislation to protect the privacy of consumers' online data by improving transparency, strengthening consumers' recourse options when a breach of data occurs, and ensuring companies are compliant with privacy policies that protect consumers.

###

Permalink: https://www.klobuchar.senate.gov/public/index.cfm/2019/6/klobuchar-murkowski-introduce-legislation-to-protect-consumers-private-health-data

# Don’t Count on Government to Protect Your Privacy

Let’s look to technologies like blockchain and other innovations to keep our data private.

**By Kevin McCarthy**
Mr. McCarthy is the House minority leader.

July 14, 2019

Imagine that Congress proposed a law that made postage free in the United States. Even in the digital age, this would be quite convenient. The only catch? In exchange for free mail, postmasters would be permitted to open your mail and read our letters and bills. The benefit, postmasters would insist, is they would know when you’re planning a family vacation. And then the post office could send you hotel recommendations or advice for the best restaurants and activities.

Convenient, right?

On second thought, you might rather pay the 55 cents for postage if it meant keeping advertisers from knowing the location and itinerary of your family vacation before you even get on the plane.

We prefer that strangers not read our mail — that’s why we’ve made doing so a federal crime punishable by up to five years in prison. We have blinds because we don’t want outsiders peering into our homes. We have laws to protect our health care records because we definitely don’t need strangers knowing our medical history.

So why should we treat our online identities — and privacy — any differently?

The answer to this question — posed by my friend Tom Siebel, a tech entrepreneur — clearly is that we should not. But if we are to secure our data in an increasingly digital world, should we expect government to singularly and effectively do the job for us? I would argue, no.

Some politicians, primarily those running for president, have called for brute government intervention, including breaking up big companies like Google or Facebook. This clarion call has the benefit of simplicity, but has failed to explain how it will increase security for our data. What does forcing Facebook to sell WhatsApp have to do with Facebook or WhatsApp collecting, exploiting and selling our data?

Others are calling for invasive congressional regulation. But as history tells us, overly broad and indiscriminate regulation often insulates the incumbents and boxes out the upstarts and smaller firms — a consequence we’ve experienced with the Dodd-Frank

financial regulations law. Even Facebook's chief executive, Mark Zuckerberg, acknowledged this possible outcome to Congress a year ago.

Unsurprisingly, these remedies lean on the premise that only government can solve market inefficiencies that lead to irresponsible corporate behavior.

I don't think we should feel confident that the bureaucratic leviathan has what it takes to develop or enforce nimble responses to rapid change in the technology industry.

We should look instead to the greatest driver of competition, the free market, for the most compelling responses to our privacy concerns.

Technological advancements can meet Americans' demands for privacy, and perhaps already are, through cryptonetworks. Cryptonetworks are decentralized platforms governed by the community of users rather than by chief executives or small management teams.

You would access these networks by logging on to a browser similar to what you use today. But the piping undergirding the decentralized networks is powered by blockchain technology capable of delivering stronger data security, portability and privacy for every user.

When you purchase or post something on a blockchain platform, the network will verify your identity using an encrypted key that is permanently and exclusively yours. Each action is recorded on a distributed ledger. This will make fraud nearly impossible.

Under the current internet framework, users' data is usually controlled by the platform — online consumers leave a trail of data bread crumbs, making us vulnerable to privacy invasions. In a decentralized network, however, our data would be controlled by this blockchain. Users would grant and revoke access to data, no longer entrusting third parties or tech companies with that responsibility.

Furthermore, this technology would increase competition, because blockchain makes it easier for anyone to create an alternative platform for communicating or providing some service. With the open-source nature of blockchain technology, a community of users is free to take what they like from an existing platform to a new one if they feel their privacy has been infringed or trust violated. Accountability is built into the system.

Each new platform is a fresh opportunity for users and creators to interact, shop and communicate without Big Brother or Big Tech tracking every move.

In many respects, it is a throwback to the permission-less innovation that brought us the internet we know today. For the free market, there is no better remedy to monopolistic behavior.

That is not to say that there is zero role for government. The Federal Trade Commission should step in when companies break the law or violate settlements with consumers or the government. Indeed, the F.T.C'.s role is perhaps more important and challenging than ever, because big tech continues to grow bigger.

Congress also has a role. It should develop a clear privacy framework that sets one federal standard for the country and adheres to three simple principles: You should be able to see, control and delete your data. These standards have the advantage of being bipartisan, which in today's Washington is saying something.

While the obscurity of blockchain might make it seem intimidating, we are seeing leading technology companies and venture capitalists looking to bring it into the mainstream.

As the most technologically advanced country in the world, it is America's responsibility to give this technology space to run and grow. Companies that have repeatedly broken promises to their users deserve scrutiny. But the federal government must not mistakenly turn scrutiny into suppression.

In the right "light touch" regulatory environment, decentralized networks can provide the transparent, secure platforms that respect an individual's privacy and dignity.

Kevin McCarthy, a Republican of California, is the House minority leader.