HB619 – Written Testimony

Christina Glabas – Gazelle Consulting, LLC

March 7, 2023

Why having a strong definition of biometric data is important

It is essential that this legislation includes a clear and robust definition of biometric data as a sensitive category of data. Immature uses of biometric data are already exacerbating existing inequalities, and it is critical that covered organizations understand the gravity of having access to this data and use it responsibly.

We must take steps to ensure that organizations are fully aware of the sensitive nature of biometric data and the potential for harm if it is not handled properly.

Biometric data is unique to each individual and can never be fully de-identified or disassociated from the person. This highly sensitive data is being used by businesses to develop technologies like facial recognition without sufficient scientific or statistical rigor. Despite the sensitivity of the data and the human subjects involved, corporate research is not regulated by consumer protection laws.

This lack of oversight can have serious consequences. For example, evidence is emerging that privacy may be impossible in the metaverse due to the wealth of biometric data collected by VR technologies that include eye movement tracking, voice prints, and visual recordings of the users home environment, among many others.

We do not yet know the long-term implications of widespread use and non-consensual study of individuals' most indelible characteristics. The outcomes of their inclusion in this kind of corporate research may have profoundly negative consequences for the rest of their lives. That is why it is essential that we have strong protections in place to ensure that biometric data is used only with informed consent and that such uses are disclosed to data subjects through the privacy notice.

It is important for consumers to know the specific third parties controllers share data with, so they can actually exercise their rights

Through my work as a HIPAA privacy consultant, I can attest to how important it is that consumers be able to track exactly where their data is going. Data exposures frequently occur through chains of vendors, which we know from our exploration of the shadowy world of data brokers.

It is unrealistic to expect the first link in the chain to bear the entire burden of cybersecurity, and we must distribute responsibility and accountability to parties that have access to and benefit from this data. Failing to provide transparency to consumers regarding third and fourth party access will limit their ability to exercise their rights. At the end of the day, while companies like Experian may be third or fourth parties to the originator of the data, they are first parties to the people they sell it to, and consumers should have rights with respect to these transactions.

Close out

It has been an a honor to participate in the development and revisions to this bill. This is a fascinating field of technology, law, and business and I deeply appreciate AG Rosenbulm's support in making sure that Oregonians have the cutting edge privacy legislation that protect consumers by demanding transparency from those who use and benefit from our data.

AG Rosenblum, Kimberly McCullough, their team at the DOJ, and the team that they have assembled for the privacy work group, thank you all for your incredible work on this bill.

Thank you for the opportunity to speak to you all today!

(Testified verbally) - Intro

Chair Prazanski and members of the committee. Thank you so much for the opportunity to speak with you today.

My name is Christina Glabas and I am the owner and founder of Gazelle Consulting, a data privacy and security consulting firm and a member of the Consumer Privacy Task Force's Central Table. I am here to express my support for HB 619.

Collaborating with the members of the AG's Policy team and being a part of this policy workgroup has been a great privilege. The group is comprised of a diverse range of individuals, including consumer advocates, industry representatives, privacy specialists, and major technology companies who have contributed their expertise to shape this legislation.

During the development of this bill we leaned on great legislation including GDPR and privacy acts in California, Colorado, and Connecticut to guide the development of this bill, ensuring that it sets realistic expectations for businesses.

(Testified verbally) This bill is reasonable for businesses and good for consumers.

During my career I've had the privilege of working with over 90 different businesses, ranging from small clinics, to non-profits, to software conglomerates, to help them develop privacy and security programs that comply with regulations such as HIPAA, GDPR, and CCPA. Through this experience, I been a partner in the challenges and successes that businesses have in adapting to the demanding pace of technology growth.

I understand firsthand the need for this legislation to be workable and affordable, as I cannot offer my services to the small businesses that makes my work meaningful if it isn't.

What I have learned is that businesses of every size regularly lack a comprehensive understanding of their own data and technology systems, and while we can't expect every business to be a cybersecurity specialist, until their business models stop relying so heavily on consumer data they'll need to learn how to be ethical stewards of the surprisingly precious information they may have about any consumer.

There is a critical role that regulators must play in this moment. This is an important opportunity to provide businesses with practical guidance that make meaningful impacts on consumers' privacy, while allowing them to focus on their core competencies, and this bill strikes that balance.

As a privacy implementation specialist I feel this is achieved through a thoroughly designed list of requirements for the privacy notice that corresponds to the control elements of the bill and a data privacy impact assessment.

GAZELLE CONSULTING LLC