New York State Senate - Public Hearing, Consumer Privacy
Committee on Consumer Protection & Committee on Internet and Technology
November 22, 2019

Chairman Thomas, Chairwoman Savino, and members of the two committees, thank you for calling this hearing and for the opportunity to testify. My name is Zachary Hecht and I'm the Policy Director at Tech:NYC—a nonprofit coalition with the mission of supporting the technology industry in New York through increased engagement between our 800 member companies, New York government, and the community at large. Tech:NYC works to foster a dynamic, diverse, and creative ecosystem, ensuring New York is the best place to start and grow a technology company, and that New Yorkers benefit from the resulting innovation.

In my testimony today, I will discuss the importance of consumer privacy, broadly outline principles of practical and effective privacy legislation, and detail the complications that can result from ill-conceived state regulation—for businesses, consumers, and New York State. I will not specifically address S5642, nominally the New York Privacy Act, and for specific feedback on that bill, you can reference testimony I delivered before these two committees in June.

We are here today because as the Internet and other digital technologies continue to proliferate and become increasingly vital to our everyday lives, there has been a growing conversation around data privacy, in New York and around the world. There is now increased awareness and understanding of how digital technologies operate and that along with the countless benefits offered by many innovative technologies come potential privacy risks that must be addressed. To state the obvious, consumer privacy is incredibly important and individuals have a right to privacy.

What this right to privacy means in practice—in a digital context—is that individuals should have the ability to know what personal information is being collected, how this information is being used and/or shared, and to control further usage of their information; in slightly more legalistic and technical terms, users should have the right to access, delete, and port their personal information. Importantly, these rights are not always straightforward and should not be read as

absolute; we must consider how they interplay with other individuals' rights, free expression, public safety, and innovation.

In an effort to secure and protect consumer privacy, many technology companies already offer users many of these capabilities. As I have previously stated, privacy is increasingly a crucial component of commercial success and it is now a core business function for many technology companies. In addition to offering users access and control, a number of companies are now developing and deploying privacy enhancing technologies—such as federated learning and differential privacy—to continue offering innovative services while ensuring privacy.

Even though several companies are already implementing privacy solutions and offering users privacy enhancing tools, it is clear government can and should play a role in protecting consumers. As I've previously discussed before these committees, there are already several sector-specific privacy laws in the United States. Yet, in order to properly and adequately address issues of consumer privacy, we believe that the United States federal government should advance a national, comprehensive framework governing individuals' data rights. This national framework should include—at the very least—the rights I previously outlined, while also ensuring there are clear mechanisms for compliance and tools of enforcement.

At the same time, we remain concerned about state- and local-level privacy regulation. Simply put, the Internet transcends state borders and a state-by-state patchwork of regulations would create burdensome compliance requirements. If each state adopts different proposals, companies of all sizes will need to expend significant time, resources, and money to comply. This will inevitably have negative effects for businesses, New York's economy, and consumers.

The reality is that state privacy legislation could have the effect of impeding, perhaps even reversing, some of the incredible gains our state has made. In the last decade, New York State has established itself as a global leader for innovation and our state's technology ecosystem has seen tremendous growth. Global technology companies are increasingly establishing a presence here, while entrepreneurial New Yorkers are starting technology companies at a record pace. New York City alone boasts more than 9,000 start-ups, with a total valuation of over $71 billion. In total, over 663,000 New Yorkers work in tech fields and the technology sector accounts for approximately $120 billion in economic output — which is about 8% of New York's overall economy.

The difficulty and costs of compliance that would result from a patchwork of state privacy laws could also serve to benefit the largest companies and disadvantage start-ups and small businesses—negatively impacting competition and innovation. The largest companies will be able to hire compliance staff and spend significant resources reworking products and services, while small businesses will not be able to do the same. As I've discussed, we can look to Europe as a guide: since GDPR was implemented it is estimated that the amount of venture capital invested in European start-ups has decreased 50% and the market share of smaller tech companies has declined.

Beyond the potential chilling effects on our economy and innovation, state legislation may delimit the services and information New Yorkers can access; small and medium sized companies may make the determination that the compliance costs outweigh the value of serving New Yorkers. Again, we can look to Europe. Since GDPR went into effect, a number of services are no longer available in Europe and over 1,000 news sites ceased offering content in Europe. If you go to Europe right now, you will not be able to access the Daily News and a number of other well-known publications.

It is not hyperbolic to say that varying state privacy regulations could lead to a fracturing of the Internet. While we hope the federal government will address consumer privacy in the near future, we understand that in the interim, New York State will continue working to address consumer privacy. When doing so, we urge the legislature to weigh the negative externalities associated with a patchwork of regulations and to ensure that any legislative efforts take these realities into account. We look forward to having further conversations on this important issue. Thank you.