Testimony of Ryan Weber – President, KC Tech Council
March 26, 2019

United States Senate Subcommittee on Manufacturing, Trade, and Consumer Protection
Hearing on "Small Business Perspectives on a Federal Data Privacy Framework"

On behalf of the KC Tech Council, our member companies and board of directors, thank you for the opportunity to testify about the potential impact future federal privacy laws could have on small and startup tech firms. The KC Tech Council is a nonpartisan, nonprofit 501(c)(6) association serving as the regional advocate for Kansas City's tech industry. The organization is funded by regional tech employers and led by a board of directors consisting of 40 executives from enterprise level and small to medium-sized companies.

It has been my honor to serve as President of the KC Tech Council for the past seven years. My statement today has been formed by direct feedback from our member companies, board members and our federal advocacy partners at CompTIA. Although the KC Tech Council's membership includes enterprise-level companies, this statement was created on behalf of companies with less than 500 employees.

Federal Preemption

A strong, preemptive Federal Data Privacy law is essential and supported by the KC Tech Council. In a recent survey of our members who identify as small or medium-sized tech firms, we asked:

> *"In regards to your business's ability to scale, how important is federal preemption of data privacy laws rather than state-by-state laws, like California's CCPA?"* Unanimously, the response to this question was; Very Important. Below are three examples why:

Unpredictable | Often, business leaders are expected to predict the future to grow their business. The recent passing of California's Consumer Privacy Act (CCPA) sent a ripple throughout Kansas City's tech industry and the business community. It will require a business to put a conspicuous "Do Not Sell My Info" link on its website and delete consumer information upon request, among other things. As other states follow suit and amend their privacy laws, tech companies will face countless and sometimes conflicting requirements. This regulatory

uncertainty is a huge concern and a threat to small and startup companies. A reasonable federal data privacy law will stabilize this threat.

This unpredictability can affect future investment, too. According to research conducted in the first six months after GDPR's implementation, overly prescriptive privacy laws can have a disproportionate impact on small businesses. Investment in startups and new tech companies in the EU has dropped since the GDPR went into effect in May,[1] while small businesses in Europe have lost market share to large companies in places like the ad tech sector in recent months.[2] Meanwhile, some US websites have chosen to block EU visitors rather than spend the money required to come into compliance with GDPR.

Innovation | Artificial intelligence (AI), machine learning and blockchain are currently referred to as emerging technologies. These tools are complex, and only a small number of people in the world fully understand how to scale these applications successfully. The convergence of these tools with Big Data analytics helps businesses make better decisions, reduce costs and transform their business processes. Without access to this data, the continued investment in these and other new technologies may wane. As I will touch on shortly, a federal privacy law can address consumer concerns by requiring transparency and notice of the algorithms, processing, and transfer of personal data.

GDPR and CCPA address an individual user's "right to be forgotten." In theory, this principle is worthy of attention. However, in practice, business leaders are concerned about the feasibility of recalling or deleting individual user data, specifically on legacy systems. It is possible deleting records could affect the future use of a database with emerging technology applications. This is a particular concern with blockchain technology.

GDPR also contains a purpose limitation that prohibits companies from using personal data for a purpose other than for which it was originally collected. While the goal of the purpose limitation, trying to limit the use of data, is noble, the result has been that companies are prevented from using their data for developing innovative new products, machine learning or AI. The US should certainly place limits on the use of personal data, but it should provide flexibility for innovative uses as long as there is little or no risk of harm to users.

Cost | The evolving patchwork of state privacy laws places a significant legal and technological burden on small and startup companies. A 2017 Ponemon Institute Study found that the average cost of data protection compliance for multinational organizations had increased 43% from 2011, although the cost of non-compliance proved much greater.[2] The cost to build privacy-compliant

[1] Jia, Jian and Jin, Ginger Zhe and Wagman, Liad, The Short-Run Effects of GDPR on Technology Venture Investment (November 5, 2018). Available at SSRN: https://ssrn.com/abstract=3278912 or http://dx.doi.org/10.2139/ssrn.3278912

[2] Fifth annual survey shows a significant spike in legal defense spending while breaches involving third-party organizations remained the most costly https://www.ponemon.org/news-2/23

software products, websites and applications are rapidly increasing, and the more regulatory masters there are, the greater the increase.

A state-by-state approach to data privacy creates a compliance nightmare for the entire tech industry, but particularly for small businesses with limited resources. Data does not abide by state boundaries, but each state has its own privacy law for its residents. As states create new and increasingly disparate privacy requirements, the result will prove untenable and could have a disastrous impact on small businesses and innovation.

It is not common for businesses to advocate for federal regulation, but a federal standard for data privacy is simply too important. Our support for a federal law should reinforce the impact these laws have on the success of small and startup US technology companies. Without federal preemption, innovation may be slowed or altered in order to comply with state laws, and the cost to comply may put some small and startup companies out of business.

Statutory Considerations

In today's economy, personal data is a valued asset for almost every business, and for many, the most valuable asset. Using other information from data brokers, companies can now narrowly target their prospects and customers in ways we could not imagine five years ago.

In this tension between commerce and privacy, we believe transparency is key. Companies should know how they collect, use, store, secure and share personal data, and be accountable for it. We believe a federal law can embrace the principles of data privacy and still keep the regulatory burden within reason for small to medium-sized businesses.

Privacy | A federal privacy law should ensure that businesses only use personal data for legitimate purposes and disclose those uses and purposes. Businesses should not make new and different uses of personal data without consent or a similar justification. They should collect only the personal data they need, and not keep it longer than they need it. They should take reasonable measures to protect the data and have a way for people to correct inaccuracies. They should provide notice in the event of a breach.

> *"If a new federal law can help move the EU to view our privacy protections to be "adequate," we may be able to avoid some serious obstacles to data transfer and online commerce created by GDPR." – Tedrick Housh, Data Privacy attorney at Lathrop Gage, Kansas City, MO*

Collection and Use | How data is collected and used are already set forth in most companies' privacy policies and terms & conditions. In some cases, data is sold to generate revenue and sell advertisements. The process by which data is sold, and for what intent, should be transparent.

The goal of any privacy law should be to prevent personal information from being used in ways that harm individuals. New federal privacy law should not contain absolute restrictions on the collection of data or include non-personal data within its ambit. GDPR, for example, includes publicly available IP addresses as "personal data." The risk of harm to individuals from possessing these types of data is extremely low. If a company is transparent about the fact that it will not re-identify its aggregated, anonymized and/or encrypted data, and abides by that commitment, it should not be subject to the same fines and other enforcement as a company that is not transparent.

Storage | The databases used to store collected information are complicated and connected, whether on-premises or in the cloud. Some data is used often and necessary for business operations. Other data sets, without immediate or functional need, are nonetheless a source for research or technological advances. Mere storage of personal data, without misuse or lack of security standards, should not result in liability.

Security | Threats to company data are not only constant; they are constantly changing. Security is not "one size fits all." No matter who has it, sensitive data (like genetic or medical information) should be subject to enhanced protection, boosted by more frequent penetration testing, cybersecurity audits, and other measures. Otherwise, we believe companies securing ordinary personal data could be subject to a "reasonableness" standard that takes into account the company's particular industry, financial means, and size.

Portability | Data portability is a two-way street. Just as consumers increasingly expect their personal data to be portable, like a cell phone number, companies should be able to transfer such data in its possession in a merger or acquisition. So long as a company has been transparent in how it shares data with third parties, it should be able to share or sell personal data without fear of violating the law.

Enforcement

Accountability is an important aspect of meaningful data privacy law. GDPR and CCPA include predetermined levels of fines, which reach into the millions of dollars or a percentage of revenue, whichever is higher. Fines at this level could mean the end for small and startup companies. An executive from one of our member companies weighed in on this subject:

> *"The law should not be so broad that it allows big companies like Facebook or Amazon to sell personal data but not so onerous that smaller businesses incur large costs to be compliant." - Jeanette Prenger, CEO of ECCO Select, Kansas City, MO*

Another potential death blow to small to medium-sized businesses is a data breach class action lawsuit. Even with little or no proof of identity theft or other injuries to the consumer class, courts

are letting these cases proceed. A new federal data privacy law could define the type of tangible proof of actual harm to give standing before a court.

Conclusion

Algorithms are the backbone of most modern technology applications, and algorithmic thinking is necessary when considering the future of federal data privacy laws. Conditional algorithms use IF-THEN decisions between two courses of actions. For example, IF a company, no matter the size collects sensitive data, THEN it must comply with federal data privacy laws and meet certain cybersecurity standards set forth by the appropriate regulatory agency.

As technology continues to advance and find its way into every industry, business sector, and company, we must remember, not all technology is created equal and not all data should be treated the same.

Accountability will make federal data privacy laws effective. The agency responsible for upholding these laws should be allowed to adjust fines and penalties equal to the violation. This sentiment is shared by our member companies. Other global examples of privacy laws, such as General Data Protection Rights (GDPR), set fines at such a high-level many small and startup companies cannot afford.

We believe small to medium-sized tech companies are already defining and creating the jobs of the next generation. Thank you for the opportunity to present the KC Tech Council's views on how to promote that growth and respect data privacy at the same time.