TECHNET
THE VOICE OF THE INNOVATION ECONOMY

TechNet Northeast | Telephone 508.397.4358
One Beacon Street, Suite 16300, Boston, MA 02108
www.TechNet.org | @TechNetNE

November 22, 2019

Re: Protecting Consumer Data and Privacy on Online Platforms

TechNet Testimony

TechNet is the national, bipartisan network of over 80 technology companies that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50 state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents more than three million employees in the fields of information technology, e-commerce, clean energy, gig and sharing economy, venture capital, and finance. TechNet is committed to advancing the public policies and private sector initiatives that make the U.S. the most innovative country in the world.

TechNet greatly appreciates the opportunity to testify and respectfully submits these comments regarding concerns and challenges faced by consumers online, especially when it comes to safeguarding their personal information on various platforms. The technology industry invests significant resources to protect public safety, guard our operations from interruption and intrusion, and prevent the loss of capital and intellectual property. TechNet support policies that:

- Protect and promote the ability of the private sector to be fast and agile in detection, prevention, mitigation, and response to ever-changing threats.
- Ensure the confidentiality, integrity, and availability of information networks and data.
- Provide strong safeguards to consumers while also allowing the industry to continue to innovate.
- Establish a uniform set of standards at the national level to avoid imposing a patchwork of policies across jurisdictions.

Cost of Compliance and Innovation

One year ago, the European Union enacted a comprehensive consumer data privacy law known as General Data Protection Regulation (GDPR). As Congress and state legislatures across the United States, including New York, consider how to regulate consumer privacy, there are valuable lessons to be learned regarding the cost of compliance to small businesses and start ups.

One recent report[1] shows that GDPR has already had a chilling effect on innovation related to artificial intelligence (AI). The report says GDPR "inhibits the development and use of AI in Europe," which puts

[1] https://itif.org/publications/2019/05/13/new-report-shows-gdpr-limits-ai-europe-recommends-steps-make-eu-more

companies in the EU "at a competitive disadvantage against their global competitors." The race is on to lead the world on AI, and we should be careful not to stifle American innovators who are hard at work in this area and other emerging technologies.

GDPR's impact on Europe's startup economy offers more cautionary tales. Since it took effect, academic research estimates that startup investments in European companies have dropped 40 percent. U.S. policymakers charged with drafting privacy legislation should ensure that the complexity of privacy requirements in any law does not effectively become a barrier to entry for new or potential innovators.

While many policymakers craft privacy legislation with some of the biggest companies in the world in mind, the reality is that startups and small businesses have limited resources to comply with complex regulations. New businesses in the U.S. already spend an average of $83,000 navigating regulations in their first year of operation, but that pales in comparison to the $3 million the average firm of 500 employees must spend to ensure they are compliant with GDPR. A federal privacy law should represent a national standard, but also provide flexibility for smaller companies and startups with resource constraints.

In 2015, 414,000 startup firms in the U.S. created 2.5 million jobs and in 2018, there were nearly 60 million small business employees. These businesses are truly the backbone of the American economy, and we should not enact legislation that would stifle their growth and ability to create jobs. That is why a key goal to guide the U.S. data economy going forward should be to have one clear privacy law.

Furthermore, a recently released report[2] analyzing the California Consumer Protection Act (CCPA) estimated that direct compliance costs for CCPA to be $467-$16,454 million over the next decade (2020-30), depending on the number of California businesses coming into compliance with smaller firms likely facing a disproportionately higher share of compliance costs relative to larger enterprises. These numbers should be a warning to lawmakers as they consider any data privacy legislation.

Conclusion

In conclusion, online privacy is a complex issue that we believe should be left to the federal government to establish a national standard that provides clarity and transparency for both consumers and businesses, and avoids creating a patchwork of state policies. A patchwork of state and local laws would create a complex and incohesive regulatory environment that is bad for economic growth and innovation. We thank you in advance for your consideration. Please reach out with any questions.

Christina Fisher
Executive Director, Northeast
TechNet
cfisher@TechNet.org
508-397-4358

---

2 http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf