National Telecommunications and Information Administration
Developing the Administration's Approach to Consumer Privacy
Request for Public Comment
Docket No. 180821780-8780-01
Document Number: 2018-20941

Comments of Arm
9 November 2018

On behalf of Arm, I hereby submit the following comments in the above captioned proceeding, Developing the Administration's Approach to Consumer Privacy. We applaud the National Telecommunications and Information Administration (NTIA) and the National Economic Council (NEC) for undertaking this effort and for the opportunity to comment on the proposal.

Arm is a global technology leader, headquartered in Cambridge, UK with a significant US presence and US headquarters in San Jose, CA. Arm's core business is providing microprocessor designs and related technology, which has resulted in Arm delivering the most widely used semiconductor intellectual property (IP) in the world. In fact, more than 70 percent of the world's population use Arm technology, which is securely powering products from the sensor to the smartphone to the supercomputer. Arm is also increasingly providing services that manage the devices Arm microprocessors end up in, as well as services that collect, organize, transport, maintain, and make sense of the exponentially increasing amount of data coming from the growth in the number and use of devices connected to the internet. As such, Arm has a significant interest in ensuring consumers have trust in how companies collect, utilize, and protect their data. We therefore are pleased the US federal government is looking at ways to improve and harmonize transparency, control, and ultimately trust in consumer data practices.

In general, we believe the US sectoral- and sensitivity-based approach, and reliance on the Fair Information Practice Principles (FIPPs) has been a successful approach to consumer privacy. Given that, we believe the privacy outcomes set forth in section "A." of the request for comment are appropriate as they largely mirror the intent of the FIPPs. Simplicity and clarity for consumers should be a priority for federal action as well, which is captured in these outcomes.

We would urge NTIA and the federal government to consider the impact artificial intelligence (AI), machine learning (ML), and other data intensive technologies that are just beginning to enter the marketplace will have on consumer data privacy as this work goes forward. The advancement and more widespread utilization of AI/ML is likely to change the way companies and individuals think about using data. In a fully developed AI world we will be hoping for AI machines to be able to interrogate data, and come up with useful results, in ways we may not have yet thought of or predicted. This may mean that some of our current data protection concepts may need rethinking and reframing, particularly if they could impede significant benefits to society or individuals. These could include looking at elements like detailed explicit consent, use of anonymized data, length of time data can be retained etc. At the same time AI may well introduce its own challenges, around unfair bias, transparency of decision-making, and other related issues. A new data protection system designed today must be open to the future challenge from AI.

A.4. *Security*, A.6. *Risk Management*, and A.7. *Accountability*

Federal privacy guidance should also give more direction and considerations for third-party vendors and service providers to take into account with respect to the role they play in this process. Supply chains in this area are varied and complex. Third party vendors often handle, process, store, and analyze personal data, but with less or unclear direction on what is expected of them. While it is difficult or impossible to provide a one size fits all approach, providing security guidance and risk management options for third party vendors to consider would clarify the responsibilities of those entities in the data protection process.

Further, while not explicitly contemplated in this request for comment, Arm fully supports NTIA's other work around security. Personal device and IoT security are imperative to protect consumer privacy and that work should be continued and viewed as complementary to this work.

As importantly, we believe the goals set out in section "B" are the correct outcomes for which to strive.

B.1. *Harmonize the regulatory landscape*

This is an absolutely necessary outcome of any new federal privacy framework. The internet was created, as were the countless services and applications powered by the internet, without regard for geographic boundaries. Americans should not be offered different privacy protections based on where they reside within the country, and similarly, companies should not be expected to offer different privacy protections based on where the customer whose data is being utilized resides within the United States.

Further, for the development and benefits to be realized of emerging technologies such as artificial intelligence (AI) and machine learning (ML) for example, companies will need to be able to utilize large data sets; if companies are forced to fragment data sets by state or geographic regions, it is impossible to know how limiting this may be as data sets will inevitably be smaller and less complete. The real promise of these technologies is the ability to make correlations across vast swaths of data. Harmonizing how companies can do that through a single, federal framework will undoubtedly lead to better outcomes from these technologies. Lastly, as the US government interacts with foreign governments on these issues, maintaining a single US federal standard for consumer privacy will lead to better outcomes and strengthen the US federal government's position in all forums.

B.2. *Legal clarity while maintaining the flexibility to innovate*

This outcome is also essential to ensure continued innovation and development of new technologies such as AI and ML, as discussed above. While many AI/ML applications will not rely on consumer data, many will, and flexibility and legal clarity will be essential to ensure companies can continue innovating in the US in these areas. It should be an top priority to maintain the balance recognized in this section of the request for comment.

B.3. *Comprehensive application*

This outcome is important for several reason, not least of which is the clarity it will provide to consumers. Consumers are unlikely to recognize the regulatory distinctions between various companies in the technology and internet ecosystem that have historically been regulated by different entities. The FTC should have authority to

oversee privacy protections for all private sector organizations not subjected to sectoral laws.[1]

B.5. *Interoperability*

Reducing impediments and barriers to the movement and flow of data is an important objective of the US government. The European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) receive significant attention, however there are many more geographically focused "security" requirements imposed by governments that restrict the flow of consumer data out of a geographic territory. This balkanization has the potential to undermine many of efficiencies internet enabled technology and services seek to provide.

B.7. *FTC enforcement*

With a significant track record, and decades of work in the area, the FTC is the appropriate federal agency to enforce consumer privacy for all entities described in B.3. above that are not subjected to other laws.

Again, Arm appreciates NTIA's work to drive a single, US federal framework for consumer privacy and stands ready to work with you as this process moves forward.

Respectfully Submitted,

Vince Jesaitis
Director, Government Affairs
Arm
www.arm.com

[1] This should be the case regardless of the outcome of the challenge to the Federal Communications Commission's *Restoring Internet Freedom* Order.