November 8, 2018

From: Varex Imaging Corporation
Albert Stopniewicz, Data Privacy Officer and Ethical Compliance Manager
1678 South Pioneer Road
Salt Lake City, UT 84104
Albert.Stopniewicz@varexima•ing.com
(801) 978-5406

To: National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Attn: Privacy RFC
Washington, DC 20230

Subject: **Response to Request for Public Comments**
Reference: Docket No. 180821780-8780-01

Varex Imaging Corporation hereby submits its comments regarding the above-referenced Request/Docket. Any response to this document should be directed to the undersigned.

Instead of addressing all the points and questions listed in the request we have opted for more general format to point out the main areas of our interest and concern.

The following are seven (7) groups of issues we would like to see addressed in any Federal Action pertaining to privacy protection:

1. **Domestic Harmonization of Standards and Regulations**. Any harmonization would have to take into account all applicable sectoral laws to avoid possible conflicts of law and to allow subsequent superseding and/or supplementing of those laws by a comprehensive regulation with the ultimate goal of creating a Uniform Privacy Code that could be adopted as state laws.

What the industry would also like to see is a publication of clear and comprehensive implementation guidelines to accompany the new law. The best examples would be (a) a series of publications put out by the U.K. Information Commissioner's Office (ICO), and (B) the guidelines provided by the EU's Article 29 Working Party.

2. **Harmonization with Foreign Privacy Regimes (Interoperability)**. One of the major challenges for any US-based organization conducting business globally is lawful transfer of

personal data. To that end, we would welcome a Federal Action resulting in a privacy regime compatible with privacy legislations emerging across multiple jurisdiction, mostly in EU and Asia. Any such domestic privacy regime should incorporate main principles of the EU GDPR and the OECD guideline with the goal of facilitating the finding of equivalency by the EU privacy and data protection authorities.

3. Methodology. We fully support development of methodology based on risk modeling and outcome determination analysis. In order to do that, the desired outcomes will have to be articulated and defined. To that end, creation of an advisory body representing business community, privacy experts, consumer protection agencies, law enforcement and the government would be fully supported by the community of privacy professionals.

4. Data Protection Officer. Any Federal Action should mandate appointing a person responsible for organization's day-to-day privacy protection operations ("Data Protection Officer" or "DPO") at any business organization. The EU GDPR model, which provides both regulatory of statutory authority to a person assigned to that role as well as specifically defined protections against retaliation, could be duplicated. Ideally, a DPO should also be 'deputized' by a federal agency charged with the enforcement of privacy protection to serve as its representative on the ground. It would also lend the position a stronger standing within business organization.

In addition, the regulation should create a framework for the DPO to have a direct reporting line to the Board of Directors as well as the operational independence with regard to day-to-day operations of the privacy program. As it is the case with many other legal compliance areas, absent such independence, a privacy compliance is subject to operational pressures which often results in lack of funding and deterioration of controls and processes.

5. Scalability. The proposed methodology of drawing a distinction between organizations of certain size and role in the accrual of liability for noncompliance has been tried in EU. The resulting enforcement regime had proven to be less-than-perfect and was subsequently revised to reduce distinctions between what the EU regulators termed as the roles of 'processors' and 'controllers'. Additionally, by building-in a mechanism that significantly reduces the risk of an enforcement action against smaller entities runs counter to the basic notion of justice. The scale-related distinction should be made in the assessment of penalties rather than in modulating the sensitivity of the enforcement action triggers.

6. National Certification Standards. We would support creation of a national standard certification of compliance. It would significantly improve ability of businesses to uniformly implement any privacy rules stemming from the Federal Action. It would also allow to incorporate flow-down requirements in commercial agreement without added cost of validation and verification of the implementation.

7. Consultation with Enforcement Agency. We support inclusion of a process allowing business organizations to reach out to and obtain opinion from the enforcement agency regarding specific implementation and possibility of an enforcement actions based on a particular set of facts. Any such consultation language would also need to include the 'safe haven' provisions ensuring that the inquiry would not trigger an investigation.

Thank you for giving us an opportunity to contribute to this effort. Varex would like to participate in any future consultations regarding privacy issues. Please let us know if you need any additional information or clarification.

Best regards,

Albert Stopniewicz