Dear Friends,

Happy to connect to you on the occasion of Data Privacy Day 2016. This has been an eventful year from data privacy viewpoint. We witnessed landmark data breaches like the Office of Personnel Management (OPM) and Ashley Madison, among others. With technology platforms expanding, such trends are set to continue in 2016 and businesses and governments will need to respond appropriately. Associated cost of data breaches is rising as the reputational damage and remedial requirements are more serious than the immediate financial loss.

Globally, the data protection regime continues to evolve. Realizing the pressing need, United Nation appointed its first-ever Special Rapporteur on the 'Right to Privacy'. Many countries are enacting Data Privacy Laws, while some are sharpening existing legislations through necessary amendments. There has been a surge in countries implementing mandatory data breach reporting obligations. Citing Privacy concerns, some countries are resorting to 'Data or Infrastructure Localization', which could prove counter-productive to global economy in the long run. Privacy safeguards have become a regular aspect of Global Trade arrangements like Trans-Pacific Partnership (TPP), Transatlantic Trade and Investment Partnership (TTIP), World Trade Organization (WTO) and more and also in regional arrangements such as Regional Comprehensive Economic Partnership (RCEP).

From Privacy frameworks standpoint, most noticeable development of the year was the invalidation of the long standing Safe Harbor arrangement for personal data transfer between EU-US by the EU Court. This took the technology world by storm. Both sides are required to come up with a solution that can stand scrutiny of the EU Court by this week, else all personal data transfer between parties in these regions would become legally invalid. In a contrasting ruling, EU court also decided in favor of an employer organization stating that companies can monitor workers' private online chats through their networks, even if it violates right to keep chats private.

Meanwhile, EU also rolled out the General Data Protection Regulation (GDPR) which is enforceable by 2018. The groundwork on GDPR started in January 2012, with EU commission proposing reforms to make Europe fit for the digital age. Rather than modifying the trans-border data flows, GDPR calls for stricter norms for data flow from the EU to rest of the world. On a related note, EU India FTA talks have resumed after a gap of around 18 months, and data protection and personal data transfers continue to be topically debated.

Research firm Forrester highlights that 'Privacy will be to organizations in 2016, what websites were to companies in 2000'. Gartner survey states that organizations are investing in location-based services (31%), wearable IT (31%) and behavioral advertising/digital engagement (29%), clearly hinting at technology becoming invasive. It also states that by 2018, 50% of business ethics violations will occur through improper use of big data analytics. Silver lining is the constant rise in salaries of Privacy executives, as per an IAPP survey. Organizations are recruiting professionals with specific privacy skill sets for all roles, a trend which will not only continue, but will get stronger.

In India, last year UIDAI was challenged on the grounds that the move to collect information from individuals and sharing sensitive personal information without consent is a violation of the right to privacy. The government has so far contended in the court that right to privacy is not a fundamental right under the Constitution.. The court decision will be a potential game changer for privacy regime in India.

DSCI worked with Bureau of Indian Standards (BIS) to host ISO/IEC JTC 1/SC 27 Working Group (WG) meetings during 26-30 October, 2015, in Jaipur. Out of 310 delegates from 32 countries, Indian delegation was the largest with 85 participants. It is important to highlight that Indian delegation proposed formulation of two new standards – 'Privacy in Smart Cities' and 'Privacy in Smartphone Applications,' which was well received by the global delegates. Indian experts are also playing important role in development of other privacy related standards at ISO including User friendly Privacy Notices, Privacy in IoT, Privacy in Identity and Access management among others.

Alongside, DSCI capacity building efforts in Privacy has witnessed over 400 professionals certified under DSCI Certified Privacy Lead Assessor (DCPLA©) and DSCI Certified Privacy Professional (DCPP©) and further gaining traction.

We at DSCI are of the firm view that a robust regulatory framework is the need of the hour. We have been working with Government agencies and industry representatives in order to strengthen the cyber security and data protection regime of the country.

I look forward to your enduring support in getting India recognized as a leader in privacy protection in the world.

Nandkumar Saravade

CEO, Data Security Council of India