MARCH 2019 • Vol. 4 • Issue 12
MONTHLY • Pages 64
₹ 200

RNI No.: DELENG/2015/67140; Published on: Every month; Posted at Lodi Road HPO, New Delhi on 9-10th of every month

THE AWARE CONSUMER

www.theawareconsumer.in

IN FOCUS
Forces That Will Shape The Future SMART CONSUMERS

RESEARCH FEATURE
Securing Consumer Trust In The Internet Of Things

TRUSTED SMART PRODUCTS

What consumers want and need from a connected world and how important it is to put them at the heart of the development of these digital products and services.

PLUS REPORT • MY MARKET • THE LAST MILE

VIEW  POINT

BEJON KUMAR MISRA | bejonmisra@consumerconexion.org

Shaping A Trusted DIGITAL FUTURE

THE CONSUMER MOVEMENT marks 15th March with World Consumer Rights Day every year, as a means of raising global awareness about consumer rights and their responsibilities. Celebrating the day is a chance to retrospect and plan for the future on critical issues confronting the Indian Consumers and the Industry on the need for urgent policy matters in the interest of development and growth. It also facilitates to speak up jointly with all the stakeholders to protest against market abuses and social injustices which undermine the rights of the consumers.

Consumers International has announced that the theme on the occasion of World Consumer Rights Day 2019 will be 'Trusted Smart Products'. Smart products are connected to the internet and receive, collect and send data globally. There are currently 23.1 billion smart products in the world, outnumbering people three to one. From smart phones to wearable fitness trackers, to voice-activated assistants and smart TVs, many of the products we use are increasingly becoming connected by default. Networks of smart products can also be known as the Internet of Things (IoT).

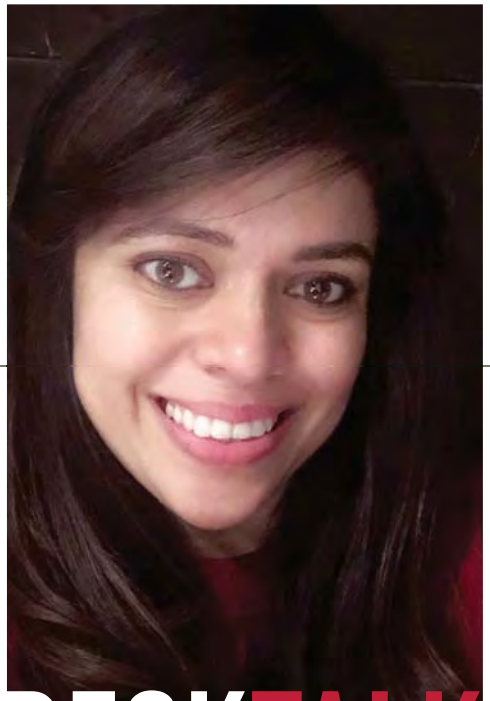
As more people come online across the world and our connection to the internet becomes better and faster, smart products will become more of a day-to-day reality for consumers everywhere, marking a major change in the way many consumers interact with products and services.

Consumers International has announced that the theme on the occasion of World Consumer Rights Day 2019 will be **'Trusted Smart Products'.**

The emergence of smart technology brings many opportunities for consumers; access to new services, more responsive products, greater convenience and choice.

As more types of smart-by-default devices and services become more mainstream, data security and privacy issues are multiplied and questions about how algorithms direct our choices as consumers are raised. The consumers want clear standards for consumer protection in theInternet of Things to remove the uncertainty and lack of protection for many connected products; consistent and effective data protection across borders; easy ways to switch between systems and providers; and clear lines of responsibility if data is lost.

As technologies continue to develop rapidly, digital transformation is pushed in new and unpredictable directions. Consequently, policymakers must react to create flexible, forward-looking and integrated policy responses that are holistic and impactful. Together, governments and stakeholders must shape a common trusted digital future that makes the most of the immense opportunities that digital transformation holds to improve people's lives and boost economic growth for countries at all levels of development, while ensuring that nobody is left behind.



DESKTALK

Message from the Editor-in-Chief

POOJA KHAITAN
pooja@jagograhakjago.com

A Complex Ecosystem

THROUGHOUT TIME, HUMANS have sought to amplify their potential through technology. We have always created tools that allow us to do more – be it the first flint hand axe, the Archimedes' lever, the printing press or the internal combustion engine. But nothing compares to the amplification of human potential that digital technologies are bringing about in the early 21st century.

Today, we have created a complex ecosystem of man, machine and software created 'Smart Products' that has transformed our daily lives –how we work, what we consume and how we travel. Smart products are even affecting relationships among people, sometimes changing how we feel about ourselves or see our place in the world.

We face a future of limitless possibilities.

As digital consumers we have an unprecedented choice of products and services. We can manage every aspect of our lives – from our money to our health – more efficiently than ever before.

Consumer skills are expected to be improved and the level of consumer awareness and engagement increased.A customer service reformation is taking place. It's radical, it's far-reaching and it's being driven by customers.As humankind continues to march towards an elusive and illusive utopia of technological advancement, the personal touch of the brand experience is fast becoming a thing of the past. While it cannot be denied that the modern methods of marketing are leaving no stone unturned in 'connecting' with the customer, but, ironically enough, it is the 'customer connect' itself, which is getting lost in the process.

Modern marketing in general, and it's digital avatar, in particular, are creating what can be called an 'imaginary intimacy' with the customer. The poor Alice-like customer is being led into a Wonderland of false promises. The clueless customer is being hoodwinked into believing that the gadget on his palm or his lap or his desk or around him (smart products) is the repository of remedies for all maladies. The biggest demerit of the digital revolution is that it has reduced consumer behaviour to a set of split-second reflex actions. The 'thinking consumer' is an endangered species now.

INSIDE

THE AWARE CONSUMER | MARCH 2019

Trusted Smart Products

"Technology enables service providers to make the location of their customers the location of their business".

RESEARCH FEATURE

17 | Securing Consumer Trust In The Internet Of Things

Consumer Applications in the internet of things can bring social and economic benefits to people around the world including: more responsive services; shorter feedback loops; remote fixes; greater convenience; decision making support; better allocation of resources; remote control of services and insights into behaviour.

HORIZONS

28 | BUILDING A SAFE DIGITAL PLAYGROUND

"By 2023, the connected play space is expected to increase 200 per cent in the next five years to $18 billion dollars." Digital Expert Xanthe Couture explores the ways children can benefit from digital technology without the risks.

GOVERNMENT PERSPECTIVE

29 | SMART TECHNOLOGY: IS INDIA UP FOR THE INTERNET OF THINGS CHALLENGE?

The Indian govt can realise the dreams outlined in the 'Make in India' and 'Digital India' missions through sophisticated IoT technology. The Indian IoT market is estimated to reach $15 billion by 2020 and will constitute 5% of the global market.

THE AWARE CONSUMER
UNLOCKING CONSUMER POTENTIAL
www.consumerconexion.org

MARCH 2019 • Vol. 4 • Issue 12

Bejon Kumar Misra
PUBLISHER
Address: F - 9, Second Floor, Kailash Colony, New Delhi - 110048
E-mail: bejonmisra@consumerconexion.org

EDITOR-IN-CHIEF
Pooja Khaitan

EDITORIAL CONSULTANTS
Praful D. Sheth
Bina Jain
Suman Misra
Manisha Bhatla
Pyush Misra
Shashank D. Sudhi
Shashi Bhushan

MANAGER CIRCULATION
Nirmal Dayal

DESIGNER: Galaxy
DESIGN CONSULTANT: Maanav Khaitan

WEB DESIGNER:
Manish Mohan
Ebrahim Bhanpurawala

The AWARE CONSUMER
is printed and published by
Bejon Kumar Misra
at F - 9, Second Floor, Kailash Colony, New Delhi - 110048 and printed at
M/s. Swastika Creation
19, D.S.I.D.C. Shed, Scheme 3,
Okhla Phase II,
New Delhi - 110020

Place of Publication: B - 306, First Floor, C.R. Park, New Delhi-110019

For any queries, please contact us at
pooja@jagograhakjago.com
Phone: 011-26271421/22/23

Total number of pages - 64, Including Covers

JUSTIN MACMULLAN
INTERIM DIRECTOR GENERAL, CONSUMERS INTERNATIONAL

Consumers do want to engage with new technologies and innovations, they just don't want to do it at the expense of their safety and privacy. These guidelines were built alongside manufacturers and give practical, real-world advice on how to build trusted smart products.

ROUNDUP

WORLD CONSUMER RIGHTS DAY

15 March, 2019

Trusted Smart Products

As more people come online across the world and our connection to the internet becomes better and faster, smart products will become more of a day-to-day reality for consumers everywhere, marking a major change in the way many consumers interact with products and services.

DATA BRIEFING

Globally, there are currently 23.1 billion smart products in the world, outnumbering people three to one.

OUR THEME FOR World Consumer Rights Day 2019 is ***'Trusted Smart Products'.***

From smart phones to wearable fitness trackers, to voice-activated assistants and smart TVs, many of the products we use are increasingly becoming connected by default.

This World Consumers Rights Day, we want to highlight what consumers want and need from a connected world and how important it is to put them at the heart of the development of these digital products and services.

There are, however, some significant causes for concern: lack of security, privacy and meaningful choice over how we use them, as well as a lack of clarity about who is responsible when things go wrong.There are also issues around lack of access, with millions of people globally locked out of this new technology by overly high data charges.

Recent innovations in mobile and sensor technologies allow for creating a digital representation of almost any physical entity and its parameters over time at any place. RFID technologies, for instance, are used to ground digital representations, which are used to track and geo-reference physical entities. In general, physical worlds and digital representations become tightly interconnected, so that manipulations in either would have effect on the other.

Integration of information and communication technologies into products anywhere and anytime enable new forms of mobile marketing in respect to situated marketing communication, dynamic pricing models and dynamic product differentiation models. As Fano and Gershman state: "Technology enables service providers to make the location of their customers the location of their business".

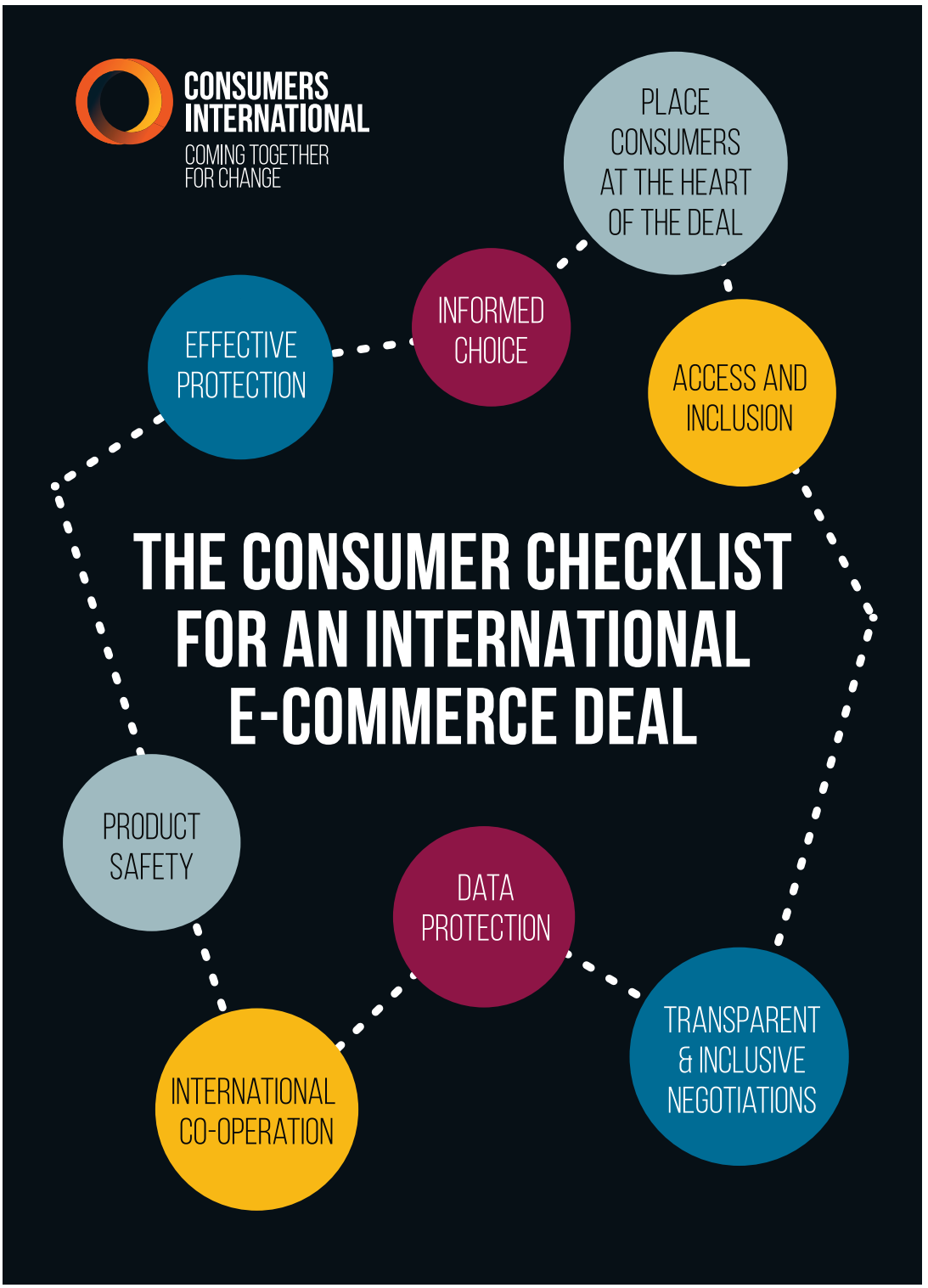
Smart products are specializations of hybrid products with physical realizations of product categories and digital product descriptions that provide the following characteristics:

- **Situated:** recognition and processing of situational and community contexts
- **Personalized:** tailoring to buyer's and consumer's needs and affects
- **Adaptive:** change according to buyer's and consumer's responses and tasks
- **Pro-active:** attempt to anticipate buyer's and consumer's plans and intentions
- **Business aware:** considering business and legal constraints
- **Location aware:** considering functional performing and restricted location choice
- **Network capable:** ability to communicate and bundle (product bundling) with another product (business) or product sets

The vision of smart products poses questions relevant to various research areas, including marketing, product engineering, computer science, artificial intelligence, economics, communication science, media economics, cognitive science, consumer psychology, innovation management and many more.

Since smart products combine a physical product with additional services, they are a form of product service system.

New Consumer Checklist Aims To Put Consumer Interests At The Heart Of E-commerce Trade Deals



PLACE CONSUMERS AT THE HEART OF THE DEAL

E-commerce would not be the success it is without the active engagement of consumers and its future depends on their trust. Therefore, an international agreement on cross border e-commerce must protect consumers and bring them real benefits.

Trade deals have the potential to deliver lower prices and greater choice to consumers and, in the case of e-commerce, measures to make it easier and safer for them to buy online. The best way to achieve this, and to ensure that consumers' interests are a focus of the agreement, is to include a chapter dedicated to consumers that incorporates internationally agreed principles of consumer protection which trade partners should follow.

INFORMED CHOICE

Consumers buying online should have information about products and services presented in a clear, accurate, easily accessible and conspicuous way so that they can make informed choices. Subscription services must clearly state when payments will be made and how a consumer can unsubscribe. Consumers should know where and from whom they are buying and have a clear understanding of their rights. Marketing and consumer reviews should be truthful and transparent.

ACCESS AND INCLUSION

The needs of marginalized or vulnerable consumers and consumers with disabilities should be considered in website design and e-commerce processes such as payments and delivery. Larger fonts and acceptable colours should be used on small screens – often the only choice for low income consumers. Responsible marketing, warnings and age verification should be used to protect vulnerable consumers.

EFFECTIVE PROTECTION

Consumers should be treated fairly and be afforded effective protection not less than the protection provided in other forms of commerce. Consumers should be able to explicitly agree to a purchase and receive a receipt. Payment systems should be secure. There should be an opportunity to return a product and receive a refund if it has not been damaged. Consumers should have easy access to fair and effective dispute resolution if something goes wrong after making a purchase online.

PRODUCT SAFETY

Products that pose a risk to health and safety should not be marketed or sold to consumers, irrespective of whether they are sold in shops or online. Product safety warnings and information on safe use, should be made clear to consumers prior to purchase. Authorities should co-operate with the Global Recalls Portal and products listed on the portal should not be sold to consumers.

DATA PROTECTON

All countries should have in place high standards of data protection and privacy in both substantive and procedural national laws. Consumers should be able to exert full control over their personal data – how it is collected, used and whether it is shared - and be able to protect their privacy. To ensure adequate enforcement and coordination, all countries should have public enforcement agencies that will work cooperatively

INTERNATIONAL CO-OPERATION

Regulators and enforcement agencies in participating countries should be encouraged to co-operate through structures such as the UN, ICPEN, the OECD and regional bodies, or in a voluntary process set up in parallel to an e-commerce agreement. Such dialogues between regulators should focus on consumer protection, and improving market surveillance, enforcement, redress and dispute resolution. Effective processes should be established for the exchange of information, conducting joint investigations, recalls and enforcement actions.

TRANSPARENT & INCLUSIVE NEGOTIATIONS

Negotiations about e-commerce should be transparent and multi-stakeholder dialogue should be encouraged nationally and internationally. Negotiating proposals and consolidated texts should also be made available to the public so that consumers know what is being negotiated on their behalf.

1 including non-monetary transactions, when consumers acquire "free" goods and services in exchange for their personal data

KEY POINTS FROM THE CONSUMER CHECKLIST

IN THE CHECKLIST, Consumers International states that any 'international agreement on cross border e-commerce must protect consumers and bring them real benefits', including greater choice, lower prices and safer digital marketplaces. See below for a summary of the key proposals:

- Inclusion of a consumer chapter: The new proposal calls for a consumer chapter to be included in any future trade deal to ensure that consumers' interests are at the heart of future trade deals.
- Five principles to follow: The chapter itself should set out the principles which trade partners should follow. These include access and inclusion, informed choice, effective protection, product safety and data protection.

Informed choice: Consumers buying online should have information about products and services presented in a clear, accurate, easily accessible and conspicuous way so that they can make informed choices.

Access and Inclusion: The needs of marginalized or vulnerable consumers and consumers with disabilities should be considered in website design and e-commerce processes such as payments and delivery.

Effective Protection: Consumers should be treated fairly and be afforded effective protection not less than the protection provided in other forms of commerce.

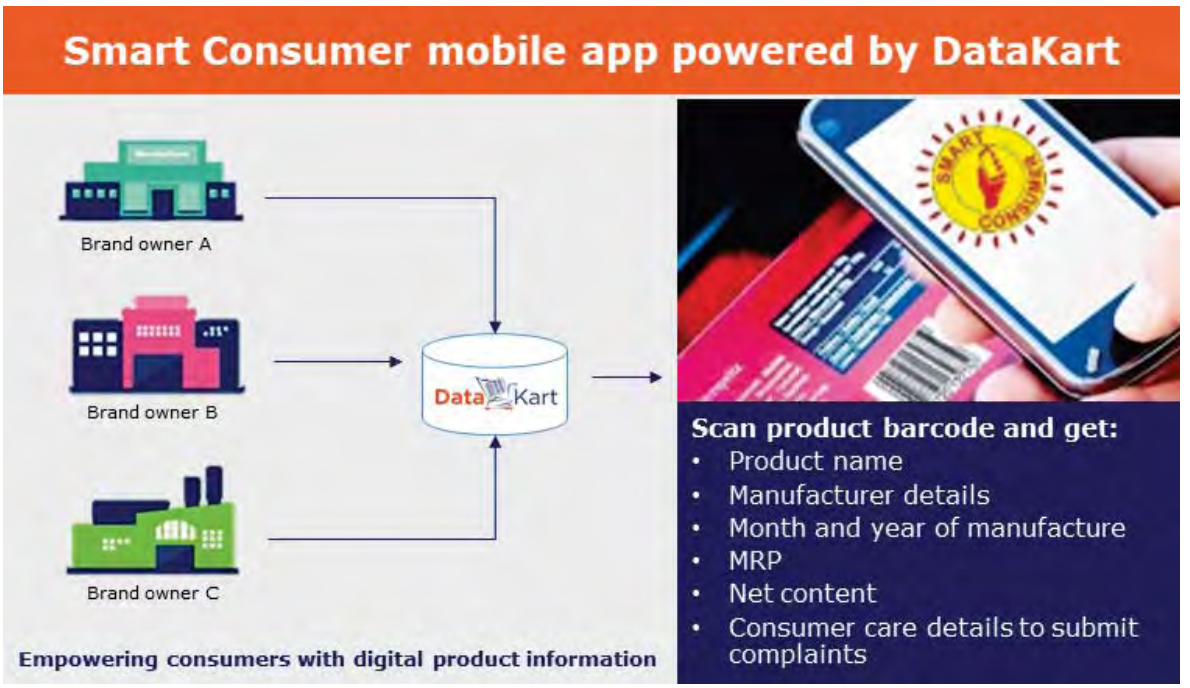
Product Safety: Products that pose a risk to health and safety should not be marketed or sold to consumers, irrespective of whether they are sold in shops or online.

Data Protection: All countries should have in place high standards of data protection and privacy in both substantive and procedural national laws.

- International guidelines and standards: Each section should incorporate relevant points from agreed international guidelines and standards.
- Encouraging international cooperation: The chapter should encourage regulators and enforcement agencies from the participating countries to co-operate through existing international organisations and networks including the United Nations, the International Consumer Protection and Enforcement Network (ICPEN) and international standards bodies to improve all aspects of consumer protection. In addition, regulators may set up voluntary co-operation networks in parallel to an e-commerce agreement.

Transparent and inclusive negotiations: Negotiations for any future e-commerce deal should be transparent, and multi-stakeholder dialogues should be encouraged both nationally and internationally, so that consumer organisations and representatives can know what is being negotiated and play an informed and active role in the process.

Powered By Datakart, The Smart Consumer Mobile App Gives Consumers Easy Access To Reliable Product Information At Their Fingertips



WORKING WITH THE Department of Consumer Affairs, Government of India, to power their Smart Consumer mobile app that helps brand owners to connect with consumers directly. The app is powered by GS1 India's DataKart.

By scanning a product's barcode, the Smart Consumer mobile app empowers consumers with digital product information on a product's name, date of manufacture, MRP, net content, along with manufacturer details and consumer care details.

Access to this marking/labelling information through the app becomes especially important when labelling information on a consumer pack is difficult to read due to its small font size. Consumers can also use the app to verify the company/product information given on the label and to connect with brands.

FSSAI compliance requirements

Through a recent circular, FSSAI requires food companies to publish their FSSAI license numbers along with products' expiry/best before date to the Smart Consumer app. This is a step toward furthering the vision of Digital India of Government of India.

AGMARK compliance requirements

AGMARK directs all its packers to comply with the Smart Consumer requirements by uploading all their product information in GS1 India's DataKart service. Read the AGMARK letter to its packers.

This is aimed at empowering consumers to authenticate AGMARK certificates on products, and hence, increasing their confidence on the use of AGMARK certified products.

Privacy And Security Guidelines For Consumer IoT Products

Consumers International, the Internet Society and the Mozilla Foundation have launched, 'Minimum standards for tackling IoT security' a short set of guidelines setting out a minimum set of requirements that industry should apply to keep connected consumer devices in the Internet of Things secure.

THE 'MINIMUM STANDARDS for tackling IoT security' guidelines have been created in response to the growing number of insecure connected consumer devices on the market and the absence of consistent, global standards. These guidelines are not intended to replace mandatory or voluntary standards that are in development. Instead, we hope they will be a useful tool that retailers and manufacturers of connected products, apps and cloud services can directly integrate, and start to phase out practices that lead to the most egregious security failings in connected devices.

Key points from 'Minumum standards for tackling IoT' guidelines:

1) Encrypted communications: products must use encryption for all of their local and network communications functions and capabilities.
2) Security updates: products must have the ability to accept automatic updates, and have that ability enabled by default.
3) Strong passwords: any non-unique default passwords must also be reset as part of the device's initial setup.
4) Vulnerability management: vendors must have a system in place to manage vulnerabilities in the product.
5) Privacy practices: Products must have a privacy policy and terms and conditions which are easily accessible, written in language that is easily understood and appropriate for the person using the device or service.

Smart products in our home

Connections between smart products and objects are rapidly expanding but unfortunately, many are rushed to market with little consideration for basic security and privacy protections. Worryingly some products are so insecure that someone with minimal hacking skills can access cameras and microphones, steal your personal information, or even communicate directly with children or adults in the house. These products can also function as a gateway to other smart devices in the home.

There is currently no effective regulation of these products, and little consumer understanding of how they function or their faults.

Connect Smart

To help consumers understand the issue and give them some practical advice about how to protect themselves, and connect SMART, together with the Internet Society, we have created some top tips.

S – search for potential security and privacy issues before buying

Search the product online for reviews or news articles that identify security

or privacy issues. Check whether you can make your device more secure by changing the password and adjusting the privacy settings. Confirm if the device receives regular software updates so any security vulnerabilities can be fixed.

M – make strong, unique passwords for each device

Generic default passwords can be easily identified and allow attackers to gain access. Set strong, unique passwords for each device, service and your home router. The longer the password the better; mix upper and lower case letters, numbers, and special characters to increase the strength.

A – adjust settings for maximum security and privacy

Many devices and services come with minimal security protection by default and collect significant amounts of important information about you – so change your settings for greater security and privacy. Also plan to reset your device regularly. If attackers do access your device, malicious code is often stored in memory and a reset will clear it. If you become aware of an incident that may affect your device, visit the manufacturer's website or contact the retailer where you bought it for information on what to do next.

R – regularly update software

If the device or app has an auto-update feature, turn it on. Find out how to check for software updates for each device and do it once a month. Most companies will release updates when they patch security vulnerabilities. Also accept updates for the apps on your mobile phone that control your device.

T – turn off features you don't need and device when not in use

Lots of features on your device can continue to monitor you even when you don't expect or need them to. To avoid this, disable cameras, microphones, or location tracking apps when you are not actively using them. And, if you are not using the device, turn it off.

5 Basic Rights The Law

A FIERCELY COMPETITIVE market comes with its own benefits – of having a choice and getting only the best, but also has its own share of negatives – of being taken for a ride way too often only for a few bucks!

To battle this, the Indian law lays down certain regulations and guidelines for protecting the consumer and guaranteeing justice.

5 important laws in this regard are:

Right to information:

Every consumer has the right to be informed about the quality, quantity, potency, purity, standard and prices of goods and services. This right is meant to protect consumers against unfair trade practices. This means that, for example, in relation to medicines, the pharmaceuticals are required to disclose potential side effects of their drugs and manufacturers should publish reports from independent product testing laboratories in order to facilitate a comparative analysis with the competitive product.

Right to choose:

Every consumer has the right to choose between a variety of goods and services. Every consumer has to be assured of an assortment of products at competitive prices. Due to the existence of this right, the formation of cartels to set up monopolies is not legal. This means that sellers of similar products or services cannot come together to form a single organization to nullify the bargaining power of the consumers. However, the reality is that such cartels do exist, and many of the closely controlled industries such as natural resources, liquor, telecommunications, etc. are controlled by a few people in power and it is believed that India has to stride for about 20 more years for empowering its citizens fully in this regard.

Right to safety:

Every consumer has the right to be protected against marketing of goods and services which are hazardous to life and property. The main application of this right is in the healthcare, pharmaceuticals and food processing sector as these have direct impact on health. It aims to protect consumers against immoral practices by doctors, hospitals, pharmacies and the automobile industry. However, the lack of world-class product testing infrastructure in the country does hamper this right to a great extent.

Right to be heard:

Every consumer has a right to be heard and to be assured that his interests will receive due consideration at appropriate forums.This right helps to empower the consumers for putting forward their complaints and concerns fearlessly and raising their voice against products or even companies and ensure that their issues are taken into consideration as well as handled expeditiously.

Right to redressal:

Each consumer has a right to seek redressal against unfair or restrictive trade practices or unscrupulous exploitation. There are consumer courts at district, state and national level for redressal of disputes. This right empowers the consumer to approach these forums and find resolutions to exploitations.

What to do if you are a victim of violation?

Laws and regulations are effective only when consumers truly understand them and more importantly, ensure their effective implementation.

If a consumer feels that he is a victim of violation of any consumer right then he can file a complaint in consumer court of India. 'Consumer Court' is the special purpose court that deals with cases regarding consumer disputes and grievances. These are

Guarantees Every Indian Consumer

"Consumer can be king only if he protects his rights as though it is his kingdom!"

judiciary set ups by the government to protect the rights of consumers. The main function of such courts is to maintain the fair practices by the sellers towards consumers.

There are 3 types of consumer courts in the country

- District Consumer Disputes Redressal Forum (DCDRF), established by the State Government in each district of the State, it deals with cases valuing up to Rs. 20 lakhs.
- StateConsumer Disputes Redressal Commission (SCDRC), established by the State Government in the State. It is a state level court that takes up cases valuing less than Rs. 1 crore.
- National Consumer Disputes Redressal Commission (NCDRC), a national level court works for the whole country and deals with amount more than Rs. 1 crore.

A consumer does not need a lawyer to file a complaint or to fight his case in this forum. He can file the complaint himself. A consumer is not required to pay any court fee but just a nominal fee depending on the type of court and the claim amount.

The procedure to file a consumer complaint:

- Firstly, identify the jurisdiction of the forum where the complaint is to be filed. The consumer has to take into consideration both the territorial and pecuniary (as stated above) jurisdiction of the tribunal in mind before filing his complaint before choosing the correct forum.
- Draft your complaint stating facts necessary to establish a cause of action. The Consumer Protection Act, 1986, contains the format of the complaint. You will be required to pay a prescribed fee along with your complaint before the respective forum.
- Attach copies of all the documents supporting your allegations. In this you can put on record the copy of the bill of the goods bought, warranty and guarantee documents and also a copy of the written complaint and notice made to the trader requesting him to rectify the product.
- You can also ask for compensation costs which should be specifically alleged in the complaint. Besides compensation, a consumer can also ask for the refunds, damages, litigation costs, and interest amount.
- You are also required to file an affidavit along with the complaint that facts stated in the complaint are true and correct.
- The complainant can present the complaint in person or by his/her authorized representative without engaging any advocate. The complaint can be sent by registered post. A minimum of 5 copies of the complaint is to be filed in the forum. Besides this you have to file additional copies for each opposite party.

National Accreditation Board for Testing and Calibration Laboratories (NABL), Gurugram

A Constituent Board of Quality Council of India (QCI), an autonomous body under the aegis of Department of Industrial Policy and Promotion (DIPP), Ministry of Commerce and Industry

NABL provides accreditation to Testing Laboratories, Calibration Laboratories, Medical Testing Laboratories, Proficiency Testing Providers and Reference Material Producers based on International Standards.

NABL accredits Medical Testing Laboratories as per the international standard ISO 15189:2012 '"Medical laboratories -- Requirements for Quality and Competence"' in the following disciplines:

- Clinical Biochemistry
- Clinical Pathology
- Haematology & Immunohaematology
- Microbiology & Serology
- Histopathology
- Cytopathology
- Genetics
- Nuclear Medicine (in-vitro)

International Recognition & Acceptance:

NABL is Mutual Recognition Arrangement (MRA) Signatory to:

- International Laboratory Accreditation Cooperation (ILAC)
- Asia Pacific Accreditation Cooperation (APAC)

New Schemes:

To ensure quality in diagnostic and healthcare services and to bring quality at every doorstep, NABL expanded its Medical Accreditation program by introducing two new schemes:

- **Recognition Scheme for Sample Collection Centre/Facility of Medical Laboratory**
- **Quality Assurance Scheme for Basic Composite Medical Laboratories (entry level)**

More than 1000 Medical Testing Laboratories have been Accredited by NABL

www.nabl-india.org

QCI
Creating an Ecosystem for Quality

Securing Consumer Trust In The Internet Of Things

Principles And Recommendations

CONSUMER APPLICATIONS IN the internet of things can bring social and economic benefits to people around the world including: more responsive services; shorter feedback loops; remote fixes; greater convenience; decision making support; better allocation of resources; remote control of services and insights into behaviour.

However, there are some causes for concern: privacy and security; lack of transparency; complex liability; lock-in to products and systems; and an increase in hybrid products which erode ownership norms, leaving consumers exposed to remote contract enforcement, loss of control and the risk of devices becoming unexpectedly redundant if support is stopped.

The potential benefits will only be achieved if services and products can be designed with trust, privacy and security built in so that consumers feel they are fair and safe to use. Working together on the following areas will be essential to building a thriving and trusted internet of things environment for consumers.

Each heading contains the main challenges and opportunities for consumers in this particular area, along with a set of principles from which specific recommendations in terms of policy, standards, testing and business practice will be developed.

1. CONNECTIVITY AND INCLUSION

As connected products become ubiquitous in people's lives, having access to a high quality, affordable internet connection, both mobile and fixed, nationally and internationally, will become even more essential for all consumers. More than ever, internet access providers shall not unjustifiably slow down, block access to, or otherwise discriminate against certain applications or services.

1.1 Consumers should have access to an affordable, high-quality, high-speed internet connection to enable them to take up the opportunities brought about by internet of things technology.

1.2 Particular attention should be given to ensuring access for marginalised or disadvantaged and vulnerable groups of consumers and those in remote or underserved geographical areas and access measures should reflect low-income groups and demographic equality.

1.3 Countries should address all drivers of affordability such as device costs and the application of unfair data caps that can keep the price of connectivity artificially high.

1.4 The principle of net neutrality should be respected.

2. INFORMATION AND TRANSPARENCY

Having the right information to understand how digital products and services work and to help make decisions is central to an internet of things environment that consumers

can trust. However, it is particularly challenging to get easily accessible, clear, concise, meaningful and verifiable information that gives full clarity to people at the right time.

Reliance on the concept of "notice and consent" alone to provide information and choice will become more problematic for consumers in the internet of things environment, given the potential for large amounts of granular data used from many different types of devices, and the number of suppliers involved.

2.1 Clear, succinct and easily understandable information about internet of things products, providers, processes and consumer rights should be prominent and readily available.

2.2 This information should enable consumers to understand the implications of their usage of internet of things products, and facilitate confident, informed decision-making. This means, in particular, informing consumers about what a product can/cannot do without being connected.

2.3 Critical information should be made prominent prior to purchase.

3. OWNERSHIP AND USE

Digital technology has changed the nature of many services and products because connected software is now contained in an increasing number of general consumer products. Established expectations of ownership are challenged in the internet of things as most products have a significant service component, or become services. They are thus subject to greater controls over use, sharing, modification and transfer to alternative services. Providers can enforce sanctions remotely due to centralised nature of their control over software and platforms and there is a lack of ability on part of the consumer to challenge sanctions or decisions made about people based on their usage. Other problems occur if the software provider changes hands and ends support for the product, or has different data governance processes.

3.1 The contractual clauses and technology that define the usage of an internet of things product or service must be fair in light of legitimate consumer expectations, with rights to fair use guaranteed.

3.2 Controls that producers can exercise over the use of a product should be legitimate, fair and proportionate, and companies should follow due process.

3.3 Depending on the nature and functionalities of a given product, it must be ensured to the full extent possible that all basic functionalities would still work without connection to the internet.

4. SECURITY AND SAFETY

The internet of things provides hackers with more vulnerabilities to exploit in more environments and, because of the high quantity of interconnections between devices and systems, potentially a faster pathway to multiple devices. Security must be ensured in all parts of a connected system, as vulnerabilities in any given component of the system can potentially compromise the whole system. Consumers will become ever more reliant on manufacturers to provide updates and maintain security.

In many jurisdictions, existing product safety legislation and standards cover the safety of individual devices but may not be fit to properly protect consumers from the security risks of internet of things as devices are part of a bigger system. To ensure the safety of the system as a whole, additional provisions and standards will need to be adopted when the device is controlled and operated as part of a wider internet of things system. This wider system also brings the risk of lower quality connection and security as more and more components and devices share frequency bands.

4.1 The concept of 'safety' in general and sector specific product safety legislation should be broadened to reflect new cybersecurity, data security and product safety concerns.

4.2 Internet of things cybersecurity measures should protect against any security vulnerability, in particular, hacking or unauthorised access and misuse.

4.3 Internet of things data and identity security measures should, among other things, protect payment details, financial assets and personal identity against fraud or misuse.

4.4 Internet of things product safety measures should protect the personal safety of consumers, reflecting the risks posed by close proximity use, shared frequency bands, the risk of electromagnetic fields exposure, and potential interference with vital connected equipment.

4.5 Consumers should not bear the risk of new advances in internet of things technology, market surveillance mechanisms should be fit for purpose and able to ensure that unsafe or potentially insecure connected products do not reach the market or will be immediately taken off the market when a hazard is identified.

4.6 Companies should adopt best practice standards such as security by design and by default, and be subject to independent assessments of compliance. In case of security incidents or data breaches, they must be subject to timely and adequate notification obligations, liability and compensation rules, and sanctions in case of neglect.

4.7 Companies and regulators should develop systems that make it easier for consumers to adopt safe and secure practices in the internet of things , for example simple settings, warnings and updates.

4.8 International standards should be developed to ensure companies provide essential security updates for internet of things products during the product's expected lifecycle for a specified and reasonable period after sale.

5. LIABILITY

The internet of things can connect devices from different manufacturers, retailers, or software developers. This complex ecosystem of connected devices can make it much harder to establish who is liable under traditional laws and regulations when something goes wrong. Additionally, many of those in the design, production and delivery chain may not have had experience of designing in security and data protection for networked devices.

A new approach to liability is required to ensure that consumers are protected in an environment where products (a) can become defective and unsafe as a result of digital security incidents; (b) increasingly take, anticipate and predict decisions without human intervention.

5.1 A clear and robust product liability framework that protects consumers if they suffer a damage caused by unsafe connected products or services is essential. As new risks arise, tort law rules governing the safety and liability standards should be introduced, replaced or updated, where necessary.

5.2 It should be clear which entity is responsible for performance and security at each point of product delivery and during the full lifespan of the connected product. Clear rules on liability should ensure that consumers are fully compensated in case they are harmed because of a defective product.

5.3 Liability rules should cover all types of products, digital content products, and (digital and other) services that comprise the internet of things ecosystem.

5.4 Liability time limits should be avoided or at least be extended to cover the expected lifespan of a product. Compensation thresholds should also be avoided to enable flexible application of awards.

5.5 There should be joint liability of all professionals in the product supply chain if their activities have affected the safety of a product. This would reflect the risk-oriented approach of product liability law and avoid problems to identify the liable person when the product is made by several producers and contributors.

5.6 Where complaints or problems involve multiple providers and/or sectors, it must be clear where a consumer should go for assistance. Alternative dispute resolution (ADR) is needed where suppliers are in different sectors, and if possible, this should have a single contact point for consumers.

6. Data protection and privacy online

Consumers should be able to exert control over their personal data and privacy preferences. It is also important to consider the impact of multiple products, services and organisations aggregating data on individuals and their rights as a consumer and citizen.

As a principle, the user or owner/user of a device should be in control of how the data it generates is used and by whom. The sheer scale of different types and amounts of data able to, not just, be collected in the internet of things , but aggregated and merged with other data poses a large risk to privacy. Objects within a connected internet of things system may collect data or information that is innocuous on its own but which, when collated and analysed with other information could reveal quite accurate knowledge of things like individuals' habits, locations, interests and other personal information and preferences, resulting in increased user traceability and profiling.

One of the most significant internet of things-related data privacy risks stems from the fact that devices are able, and indeed designed to, communicate with each other and transfer data autonomously to an external partner (such as a device manufacturer). With applications made with proprietary software operating in the background, it will become more difficult for individuals to see if, when and how processing takes place, and the ability for data subjects to exercise their data privacy/protection rights may therefore be substantially limited.

6.1 Consumers' privacy and data protection rights must be properly protected and upheld to address potential harms such as discriminatory practices, invasive marketing, loss of privacy and security breaches.

6.2 Internet of things companies and regulators should regularly review and re-evaluate the scope of personal data collection, and assess to what extent the data processed is proportionate and necessary for the service delivery.

6.3 Privacy aspects and impacts must be assessed and integrated throughout the whole conception, design and development cycle of a connected product and the networked ecosystem in which it operates (privacy by design). By default, the settings of any connected product must be set to the highest level of privacy protection from the outset (privacy by default), preventing unwanted tracking of users' behaviour and activities.

6.4 Consumers should be made aware of the implications of how data collected by internet of things products and services could be used and given simple and effective ways to assert control and mitigate risks.

6.5 Consumers' data belong to them. They must have full control over the data that stems from their connected products and their use. Companies should provide simple, secure ways for consumers to access and control their data, including the possibility to transfer their data to other services as they see fit. Consumer should be able to benefit from the economic value of their data, and other opportunities of sharing their data, in line with their preferences, expectations and legal rights.

6.6 It should be clear to consumers what data will be collected, with whom it would be shared and for which purpose it will be used throughout the duration of the product or service relationship. At the very least, connected products and services using personal data, must have a clear, comprehensive and easy to understand privacy policy in place.

6.7 It should be clear to consumers if and how algorithms used in internet of things products make decisions about them that affect the quality, price or access to a service.

6.8 Regulators should ensure the use of algorithms is lawful and does not discriminate by making detrimental decisions based on information about consumers. Regulators should consider appropriate frameworks to address problems should they arise which should include rights to challenge automated decisions that produce legal effects.

6.9 Independent, well resourced, national data protection agencies that are relevant to the internet of things should be in place. Data protection laws should be fully enforced, and strengthened if necessary where consumer detriment is identified. Given the central importance of data within the internet of things, independent data protection agencies which can fulfil their mandate to protect consumers' data are essential.

6.10 International policy on cross-border data flows should be co-ordinated so that countries involved have in place equally high standards of protection in both substantive and procedural national laws.

7. Complaints handling and redress

Interconnected services can increase convenience by removing the friction from consumer tasks involving multiple providers. However, identifying which supplier is responsible for faults or problems is complex, as is verifying claims for the quality or performance of things that rely on multiple partners in the chain to work. These complexities should not affect consumers' right to obtain redress.

7.1 Rights to redress for internet of things products and services should not be less than those available for other forms of commerce. Complaints handling and redress mechanisms should be accessible, affordable, independent, fair, accountable, timely and efficient.

7.2 Companies offering internet of things products and services should have strong internal dispute mechanisms that do not impose unreasonable delays or burdens on consumers.

7.3 Recourse to independent redress should be available to address complaints that are not satisfactorily resolved by internal mechanisms. It should be clear where consumers should go for assistance.

7.4 Where products and services cut across jurisdictions or sectors, regulators should work across jurisdictions and sectoral boundaries to support cross-border dispute resolution. It must also be clear where consumers should go for assistance.

7.5 Aggregate information with respect to complaints and their resolutions should be made public. 7.6 Online dispute resolutions should be provided but not to the exclusion of other avenues.

8. Competition and choice

If vertical integration and market concentration becomes the norm in the internet of things, it will be increasingly possible to lock people into a vendor's own products or to a closed ecosystem. This has implications for consumers wanting to shop around for different apps or services, use an independent repair service, or link to other preferred apps or data streams.

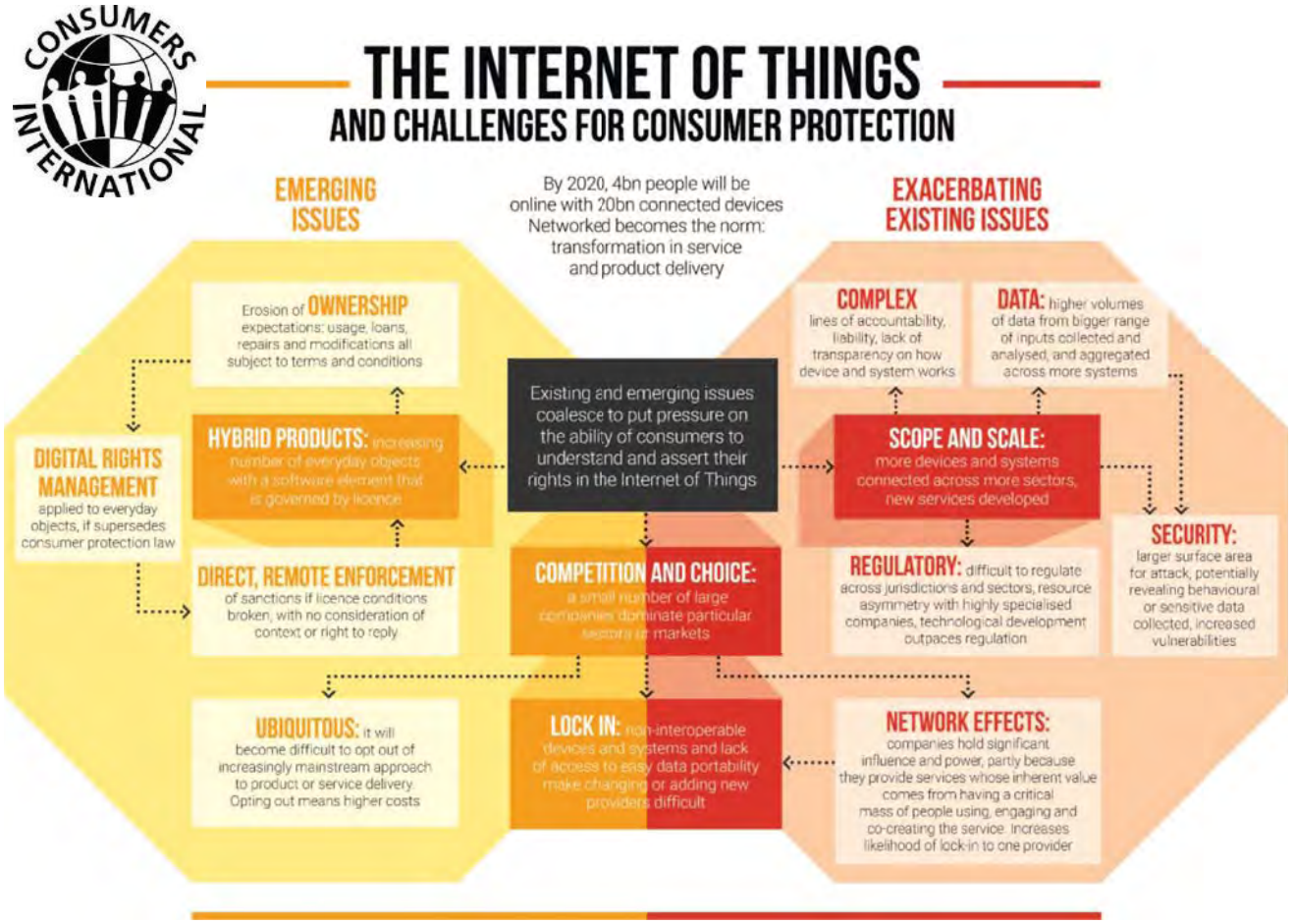
Competition law and policy should be fit for the purpose of ensuring that the internet of things is competitive in all its subsectors. Consumers often have limited rights to the data they themselves create through transactions or through using the device/service they purchased in the way they want. For example, it is often difficult or impossible to port data or content between providers. Therefore, ensuring data portability is key not only to give consumers control over their own data but to also foster competition between services. Interoperability is also an essential element to prevent consumers becoming locked into closed internet of things ecosystems. Competition authorities have an important role to play in the promotion of a dynamic, consumer-friendly environment for the development of the internet of things.

8.1 Interoperable and compatible device and software standards should be in place to avoid lock-in effects and enhance consumers' ability to easily compare and switch providers.

8.2 Transfer of data between services in order to facilitate switching should be possible whilst respecting the consumers' data protection rights.

8.3 Attention should be given to ensure that the connectivity element of an internet of things service, does not become a lock-in mechanism for consumers and that they can easily switch between connectivity providers.

8.4 Competition regulators should consider competition remedies such as requiring interoperability or access of data by competitors to mitigate the effects of data concentration and dominant players.



9. Lifecycle

Relentless innovation and competition for market-share means that the underlying technologies in devices keep surging ahead, with faster processors, better cameras, better batteries and so on. Lack of updates and discontinuation of technical support can render perfectly functional products quickly obsolete.

This means that the service life of most electrical appliances is becoming shorter. This has implications for resource use and disposal, as only a fraction of e-waste is recycled. E-waste is often highly toxic, leaching heavy metals and dangerous chemicals into the soil around landfills and releasing greenhouse gas and mercury emissions when burned. In addition, consumers are increasingly unhappy, a recent consumer survey conducted for the study revealed that about one third of those polled are not satisfied with the service life of their appliances.

9.1 Connected products need to be easily upgradeable to reduce the potential for products to be rendered obsolete.

9.2 Updates should be made available to consumers regardless of location.

9.3 As far as possible, devices, adaptors and other connection points should be compatible with each other to reduce the potential for new incompatible interfaces to render devices obsolete.

9.4 Consumers should be provided with clear, comparable and credible information concerning expected lifetime and reparability of products.

9.5 Products should be designed and built with resource efficiency in mind – from using sustainably- produced materials and construction methods; to providing clear guidance to consumers on the most efficient use, re-use/repair and disposal of the product and its components.

9.6 Products should be designed so that the time sensitive software can respond to latent or low use periods in order to save energy. Low energy products are to be welcomed.

9.7 Measures should be taken to ensure that the disposal of any heavy metals and other dangerous substances contained in connected products is not harmful to the environment and human health.

SUPPORT THE CAMPAIGN

LOOK OUT FOR THE RED LINE

BE RESPONSIBLE

Medicines such as Antibiotics have a Red Vertical Line on their pack to indicate that these should be consumed only on doctor's prescription. Always complete the full course as prescribed by the doctor.

Campaign Partners

OPPI

Consumer Connexion

Consumer Online Foundation

Healthy You Foundation

Patient Safety and Access Initiative of India Foundation
a Partnership for Safe Medicines India Initiative

SIGN THE PLEDGE.

HTTP://WWW.CAUSES.COM/CAMPAIGNS/106670-RAISE-AWARENESS-FOR-SALE-USE-OF-ANTIBIOTICS-TO-COMBAT-AMR

How Safe Is Digital India?

– Shelley Singh

UNLESS YOU ARE a hermit in the remote Himalayas, you are likely to be troubled 24x7 by thoughts of digital thefts — from personal information to financial data to biometric details.

In the recent days, weeks and months, the overdrive by the government and India Inc to link tax returns, bank accounts, mobile SIMs, mutual funds and more to the 12-digit Aadhaar has raised the billion-dollar query: Is Digital IndiaNSE 0.00 % secure? In 2016, 3.2 million credit card and debit card details were stolen by Chinese hackers.

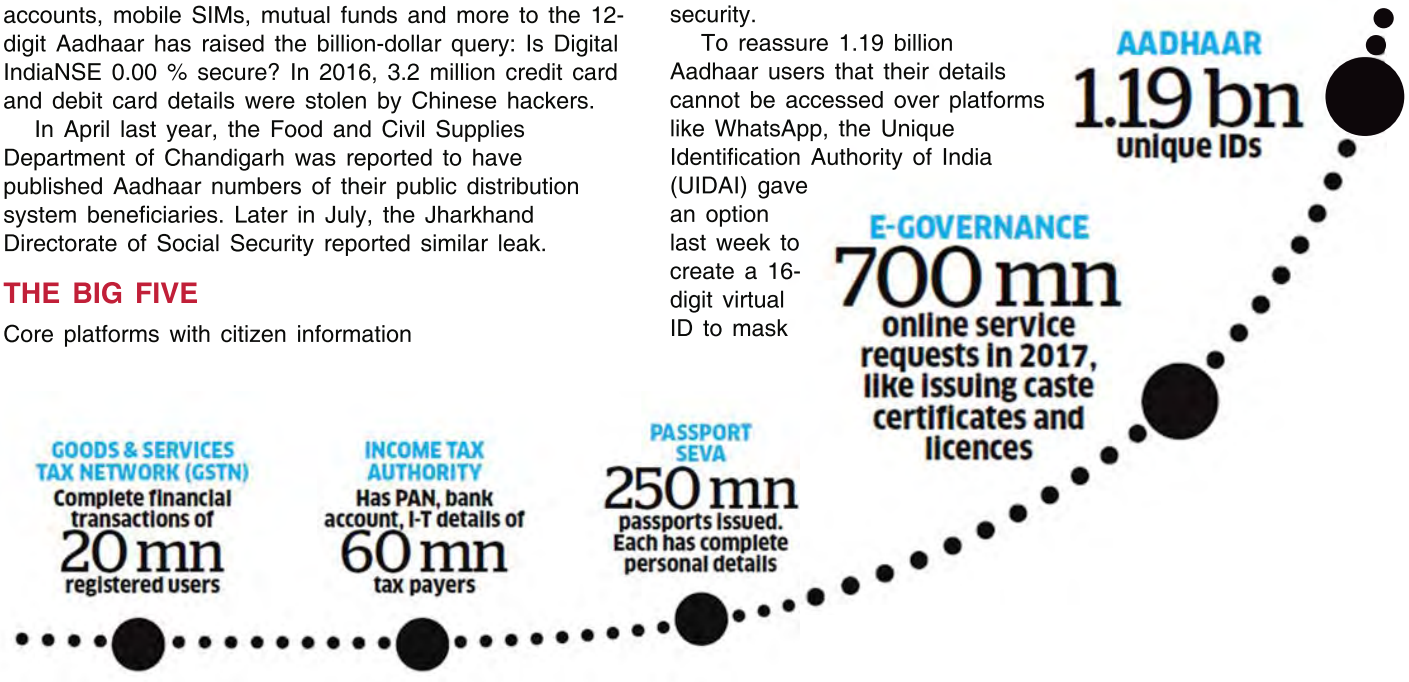
In April last year, the Food and Civil Supplies Department of Chandigarh was reported to have published Aadhaar numbers of their public distribution system beneficiaries. Later in July, the Jharkhand Directorate of Social Security reported similar leak.

American whistle blower Edward Snowden, from his asylum in Russia, and an Australian security expert Troy Hunt have raised questions on database security in India. A 2017 study by PwC and Assocham revealed attacks on Indian websites increased five times in the past four years. It noted Digital India spends miniscule amount on security.

To reassure 1.19 billion Aadhaar users that their details cannot be accessed over platforms like WhatsApp, the Unique Identification Authority of India (UIDAI) gave an option last week to create a 16-digit virtual ID to mask

THE BIG FIVE

Core platforms with citizen information



Note: Central & state government have multiple other platforms that include user details like pension records, property ownership, birth certificates

Source: PwC, UIDAI

ENCRYPTION CAN GET DATED: Most digital world is protected by encryption. Concept of encryption is that **it's irreversible but not totally secure.** For instance, banks started with 40-bit encryption 20 years back. That can be hacked in 5 minutes today. Now banks use 128- or 256-bit encryption. Aadhaar uses 2048-bit encryption. Today it will take thousands of man hours to break it, but not a decade from now

HUMAN FACTOR: There will be someone who has the master key. There could always be a **disgruntled employee who can compromise the system**

PACE OF CHANGE: In the past, an **upgrade cycle was two years; now it can be 60 days** for some software. That's faster than the time governments or private institutions often take to decide on an upgrade

MULTIPLE PARTNERS: **One builds technology with several ecosystem partners, which pose a security risk**

LAX ABOUT PRIVACY: People leave a lot of information on social media platforms and other apps **without checking privacy settings**

the real Aadhaar. In the economy's technology-driven growth story Aadhaar is the most credible identity, says Ajay Bhushan Pandey, CEO of UIDAI, which issues Aadhaar numbers.

Data Pools & Risks

There are other, equally critical data pools across Digital India platforms, with sensitive personal information about bank transactions, taxes filed, passport details, property ownership, birth certificates, photographs and so on. These reside in systems of Passport Seva, GSTN, egovernance portals, income tax e-filing, UIDAI and others. Data across systems and agencies is increasing every minute. A few lakh people apply for Aadhaar every month or go to its centres to update or correct information, including address, date of birth, name.

Sivarama Krishnan, partner & leader, cybersecurity, PricewaterhouseCoopers (PwC), says, "The government is the biggest player in digital India, with several petabytes (one petabyte is 1,000 terabytes or approximately 10 years of TV content) of data residing with various agencies. And there are multiple user agencies accessing that data to complete their tasks."

These include banks, telcos, insurance companies, credit card issuers, mobile wallets, ecommerce companies, hospitals, security and gas agencies. "Linking Aadhaar with everything is a risk if done without adequate checks and balances. Who is the actor, who owns the information, how and why do multiple agencies have access to databases? There are good uses and bad uses of data. The trouble is we don't know the bad users," says Harinder Takhar, CEO, Paytm Labs.

Paytm has a 50-strong team in Toronto to secure

Dos and Don'ts to Protect Your Data

Activate SMS alerts for all financial transactions

Avoid common passwords across platforms (like same password for bank account & Facebook)

Use strong passwords and **avoid writing down passwords**

Be careful about what **personal information you share** over the phone

When downloading free apps (or even paid ones) be aware that they **access address books and other information** on smartphones. Check if you really need them

Avoid doing sensitive transactions like **mobile banking using public Wi-Fi**

Use new tools like **Aadhaar virtual ID to mask real number**

Be careful what you print/copy on public printers (even office printers/copiers). They come with **hard disks that store whatever you have printed/photo copied**

Avoid accessing bank account, social media in cyber cafes or other people's devices

transactions for its 200 million users in India. UIDAI's Pandey, however, is less fearful, saying linking Aadhaar with everything will improve security. “When every bank account is verified with Aadhaar, every transaction will be tracked. It will make it more secure as frauds will be detected.” The accent is clearly on the cure.

Risky Yet Unavoidable

Reverting to older, time-consuming practices like paper transactions, money order transfers, queuing up in banks or writing cheques is not the answer. Reliance Jio's user base ran into millions within weeks thanks to Aadhaar ID verification. Passports are now issued in two weeks with Aadhaar from six months earlier. Tax returns are filed in real time, thanks to e-filing. Digital India will continue to expand — less than 10% transactions are digital at present. Yet Digital India needs to build trust and greater security.

The problem with government databases is that these are live, accessed by multiple users within the government and outside. That multiplies the security challenge. Saket Modi, CEO, Lucideus, says, “Every opportunity comes with a cost.” Lucideus manages security for several financial institutions, insurance companies and even the BHIM app. “No one's bank account has been compromised because of Aadhaar data leaks. As it is, the majority of non-biometric information that Aadhaar captures is already there in public domain and people share more voluntarily on Facebook and other social media platforms,” he adds.

For Aadhaar to be breached, the hacker needs biometrics as well, a near impossibility as they are securely encrypted and never shared with anyone. Biometrics-based Aadhaar has helped remove fake beneficiaries and ghost accounts. However, despite an unbreakable 2048 bit encryption of most government databases, 100% security may never be possible. Akhilesh Tuteja, head of risk consulting, KPMG India, says, “Given unlimited resources and motivation, anything can be hacked.” (See box Get Ready for Quantum Era). “Security is a journey. 100% security is a myth,” says Burgess Cooper, partner, cybersecurity, EY India.

Modi of Lucidious points out that there is more financial fraud in the US than in India (the US is also far more digital than India), yet they have not given up on Digital America. JP Morgan Chase, Visa, PayPal have all seen major cyber breaches in the past. The ratio of risk of financial fraud in the US to India is 8:1. Fraud in India has been under check due to Reserve Bank of India's insistence on the tighter, two-factor authentication and because the number of people using digital services frequently is still low. More than 50% e-shoppers still insist on cash on delivery option.

Human Factor

Some time back, UIDAI gave an option to users to mask their numbers by creating virtual identity. Chief technology officer of a bank who wished not to be named argues that while this move is great to protect identity, users have to be reasonably tech-savvy to use this. That may not be true of those at the bottom of the pyramid who get direct benefit transfer under various government schemes. Tuteja points to human risks to “secure” information pools. There could be a disgruntled employee who decides to misuse privileges.

He points to agencies' need to keep pace with the speed at which technology changes — from a two-year upgrade cycle, now it is 60 days for some software. “Technology has increased in complexity. You don't depend on one technology partner but an ecosystem of partners who supply different software. Your dependence on others is a security risk as well,” says Tuteja.

Often users store personal information on their smartphones. They download free apps like WhatsApp or TrueCaller. “These apps want to make your life easier, but at the cost of sharing your address book,” says Tuteja. An app could seek permission in its long list of conditions — which nobody cares to read — to copy every word you key in, compromising security.

Facebook and Instagram have user's name and birth dates, besides frequent updates. Amazon, Flipkart and other ecommerce companies know addresses, mobile numbers and credit card numbers. Over the next few years, if users are able to do banking via links, say, on Facebook, it will multiply risks. The biggest challenge, says KK Mookhey, founder & CEO, Network Intelligence, is “that your data is not just with your bank (or UIDAI or GSTN, etc).

There's an entire ecosystem of players and not all of them run their shops with the same level of rigour and controls that banks do.” Users need to be aware of what they do in hotspots as well. Marty P Kamden, CMO, NordVPN, a virtual private network services provider, says “Users need to be careful before connecting to public Wi-Fi.” Also, using the corner photocopy shop or even printers and copiers in offices to get Aadhaar or passport copies is not without risks. These come with hard disks that store every copy or print.

Not Enough Security Spend

Most companies still don't spend the kind of money that securing digital assets needs. For instance, JP Morgan has a $10 billion IT budget and $1 billion spend on security. Says Modi: “In India, public sector banks spend 1-3% of their IT budgets on cybersecurity and it's slightly higher in private banks vis-a-vis the US where, generally, spending 10-15% of the IT budget on digital security is a common trend among financial institutions. The US government spent $19 billion in 2017 to secure IT assets. In India, the Ministry of Electronics and IT mandated all government departments in September 2017 to spend 10% of their technology budgets on security. This was after attacks like WannaCry. The 2017 Global Cybersecurity Index by the UN ranked India 23rd among 165 countries in commitment to cybersecurity. India scored better in security than in ease of doing business, but is not entirely risk-free.

Amazon, Flipkart and other ecommerce companies know addresses, mobile numbers and credit card numbers. Over the next few years, if users are able to do banking via links, say, on Facebook, it will multiply risks. The biggest challenge is “that your data is not just with your bank (or UIDAI or GSTN, etc).

Get Ready for Quantum Era

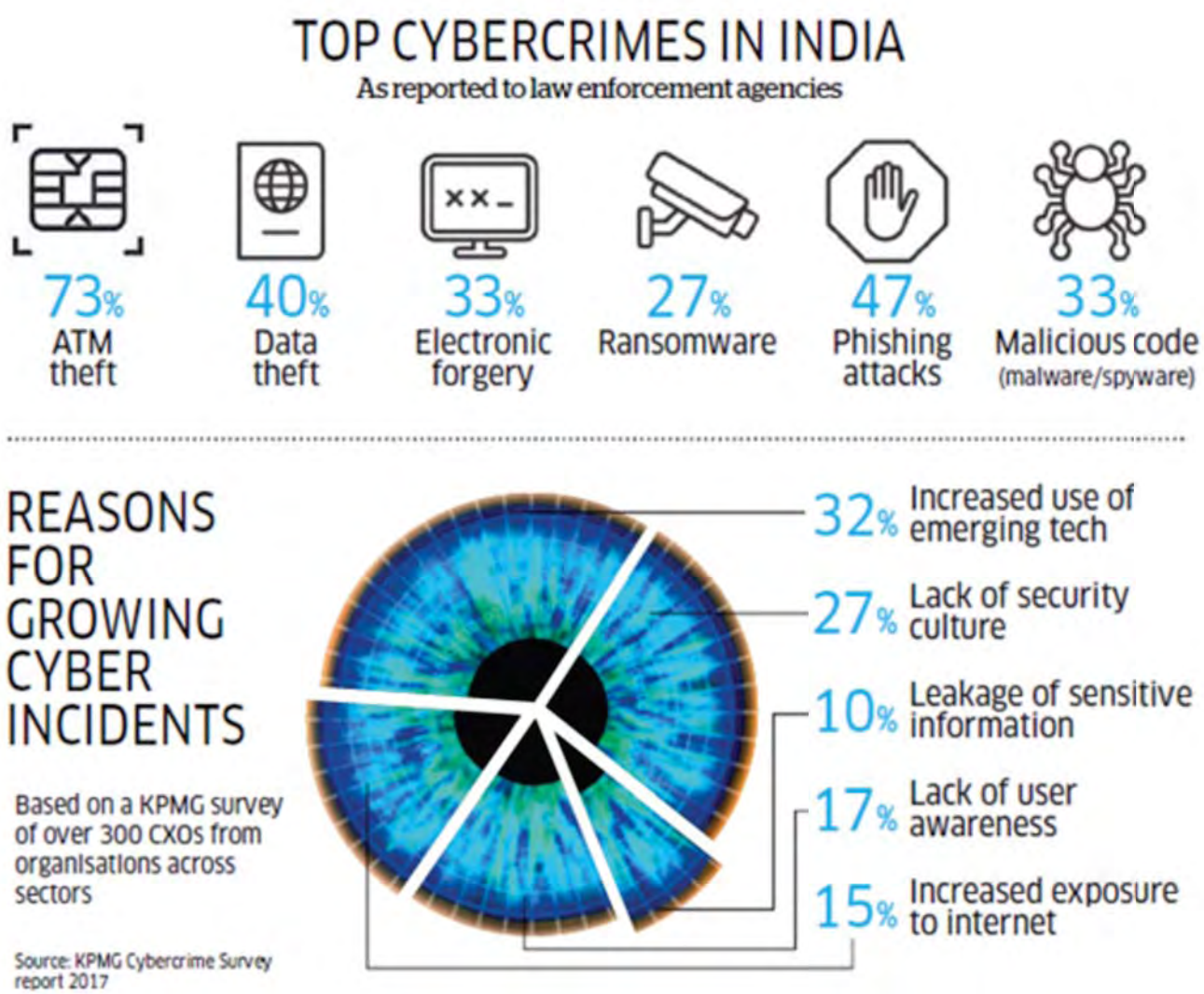
In the security world, it's a never-ending cat-and-mouse game, with hackers trying to breach networks. The greatest threat to Digital India could arise from hackers residing anywhere in the world — state-sponsored or otherwise. About 20 years back, 40-bit encryption was considered high-tech. Today it can be breached in minutes and companies have moved to 128-bit and 256-bit encryption. Databases like Aadhaar are secured with 2048-bit encryption.

“That could take thousands of man hours or several years to break,” says Ritesh Pai, chief digital officer, Yes Bank. However, what appears impregnable today could succumb to quantum computing (QC) in just a few years. “Today's encryption methods could be brought down with QC in minutes. It could become mainstream in 8-10 years,” says Harinder Takhar, CEO, Paytm Labs.

In today's computing world, information is stored in binary — 0 and 1. QC increases the ability of computers to store information in multiple bits or states. This allows them to perform incredibly complex calculations at speeds unimaginable today. Governments and companies will have to migrate to quantum era — much like how they adjusted to Y2K — and is being called Y2Q (Years to Quantum).

Even in pre-QC era, the need for quantum-safe encryption is real. Sivarama Krishnan, partner & leader, cybersecurity, PwC, says, “QC can help in enhancing response to attacks and detection capability.” While QC is a few years away, companies are evaluating blockchain which strengthens security as data resides in multiple places.

Syed Ali, principal, Bain & Company, says, “100% security is a mythical target because of the variety of attack methods, number of known and unknown hardware and software vulnerabilities, limitations in detection and response technologies, etc.” The tried-and-tested principle, adds Houston-based Ali, who lead's the firm's IT practice, “is to apply cybersecurity capabilities in layers and follow best practices for cybersecurity technologies, processes



and organisation". Perhaps move to blockchain next and be QCready soon enough.

Wanted Security Geeks

At a time when there's a hue and cry over technology jobs drying up, the software security market is staring at a crisis. There aren't enough geeks to protect digital assets. Digital India needs top professionals who can build hack-proof systems and are blockchain-and quantum-computing era ready and ensure 24x7 protection against threats. Burgess Cooper, partner, cybersecurity, EY India, says, "We talk of IT jobs going. Security is one area where there's zero oversupply."

According to technology lobby Nasscom, India is grappling to bridge the gap between demand for cybersecurity professionals and the talent pool available, with a shortfall of hundreds of thousands of skilled professionals in this domain. Nasscom and Data Security Council of India (DSCI) are planning to create a pool of half a million security professionals in line with the country's National Cybersecurity policy. Lack of security professionals is a global problem as well — an area that Indian engineers can explore. Even the US is expected to have half-a-million or more unfilled cybersecurity jobs by 2021.

Every IT worker needs to be involved in protecting and defending apps, data, devices, infrastructure and people. Cybersecurity, a complex domain with constant flux and rapid changes, wants skilled professionals having expertise in mathematics, statistics, data science and computation in order to keep up with the latest challenges in the form of attacks, crimes and frauds.

According to Nasscom, domains like identity and access management, security operations, internet of things (IoT) security, big data and cyber forensics are areas of immense opportunities for professionals in IT. Joining the Digital India army of security geeks could be the next hot spot for engineers.

Building A Safe DIGITAL PLAYGROUND

"By 2023, the connected play space is expected to increase 200 per cent in the next five years to $18 billion dollars." Digital Expert Xanthe Couture explores the ways children can benefit from digital technology without the risks.

WE WANT TO see a digital world that children and their care givers can trust. Where children feel safe online, whether it is playing with connected toys and games, finding information for school, watching videos and memes or interacting with friends and family on social media.

Despite the benefits children gain from being online, such as learning and entertainment, these online spaces can also present risks including interactions with unknown strangers and exposure to harmful content. In addition, children's use of sites and agreement to unclear terms and conditions may also result in the collection of personal data including age, location, likes, dislikes or patterns of use, which is repackaged and sold on to a multi-layered ecosystem of advertisers and ad buyers.

The design of digital platforms, from the auto-replay of videos to friendly pings of notifications, has been criticised for keeping children hooked on screens and enabling even more collection of data about them. This keeps the platforms in business but also raises persistent concerns around risks of hacking and ethical questions about the recording of play.

Unlike a physical playground, there is no consistent approach to how these risks are managed across the globe.

Consumer organisations have already taken action to improve the digital environment for children.

On a bigger stage, Consumers International is working with the international standards organisation on a new ISO standard for Privacy by Design for connected products which will include products that children use.

But there is more to be done and the work of consumer organisations in this space is only beginning.

As adults, we have more chance of taking control of how our data is used and collected, and agency to choose when we want to have digital downtime or switch off notifications. Equally, as adults, we also have the ability to decide the kind of digital world we want children to experience as they grow. The time is now to develop solutions that support and empower children in the age of ubiquitous technology.

SMART TECHNOLOGY

Is India Up For The Internet Of Things Challenge?

The Indian govt can realise the dreams outlined in the 'Make in India' and 'Digital India' missions through sophisticated IoT technology.

IN JUST A few years, the world we know has been transformed by “smart” technology. Technology that studies us and intuitively anticipates what we need. Indeed, smartphones dominate our day-to-day activities and our e-mails now write themselves. Intelligent devices such as Amazon's Alexa have become invaluable mainstays in many homes. Countries such as Sweden, South Korea, Japan, and Estonia have actively embraced intelligent technology to conserve natural resources, reduce pollution, enforce traffic control, and digitise their services. The Indian government plans to leverage Internet of Things (or IoT) technology to improve water and electricity conservation, lighting, transportation, agriculture, and access to healthcare. The Indian IoT market is estimated to reach $15 billion by 2020 and will constitute 5% of the global market. While we collect, analyse, share and store this enormous amount of data in real-time, how can we protect our privacy and information?

IoT refers to cutting-edge, intelligent inter-connected devices designed to improve the quality of our lives. This level of connectivity is a natural evolution of the internet. However, it comes with its share of concerns—particularly around the topics of data privacy and protection. Through IoT devices, the general public shares details about their personal habits by the minute. Little wonder that 97% of surveyed risk professionals were worried about cyberattacks on unsecured IoT devices as per the Ponemon Survey. After all, the world's 13th largest economy is the cybercrime market. Large-scale data breaches of Uber, Yahoo, and Facebook have monopolised global headlines. As IoT continues to make inroads into every aspect of our lives, individuals who prefer non-IoT devices will soon be unable to opt out. From household items like refrigerators and washing machines to trains, planes, and automobiles, IoT will be offered by default.

The Indian government plans to develop 100 smart cities across the nation and has allotted a budget of 7,000 crore towards this mission. Investing in IoT will bring India a two-fold benefit. Firstly, advanced IoT technology requires significant upgrades to the underlying infrastructure to support it. Improved infrastructure and driving futuristic IoT implementation will continue to maintain India as a hotbed of investment. Indian VC, Blume, created a $100 million investment fund specifically for IoT start-ups. TATA communications committed $100 million to smart cities, services and improving public safety. The most significant areas of investment for IoT companies is in utilities, manufacturing, transport, automotive, healthcare, retail, and agriculture.

So, how ready is India to embrace IoT technology and protect the privacy of its citizens?

First and foremost, the Indian Supreme Court deemed the right to privacy as a fundamental right for all Indians. Additionally, meitY (ministry of electronics and information technology) introduced the draft IoT policy that proposes an advisory committee (AC) comprising of vital stakeholders in the government, industry, and academia. This policy also introduces an IoT Program Management Unit led by a director of IoT operations and smart city support to identify new IoT opportunities, drive implementation, and track performance. It remains to be seen what level of access to data will be granted to the committee members.

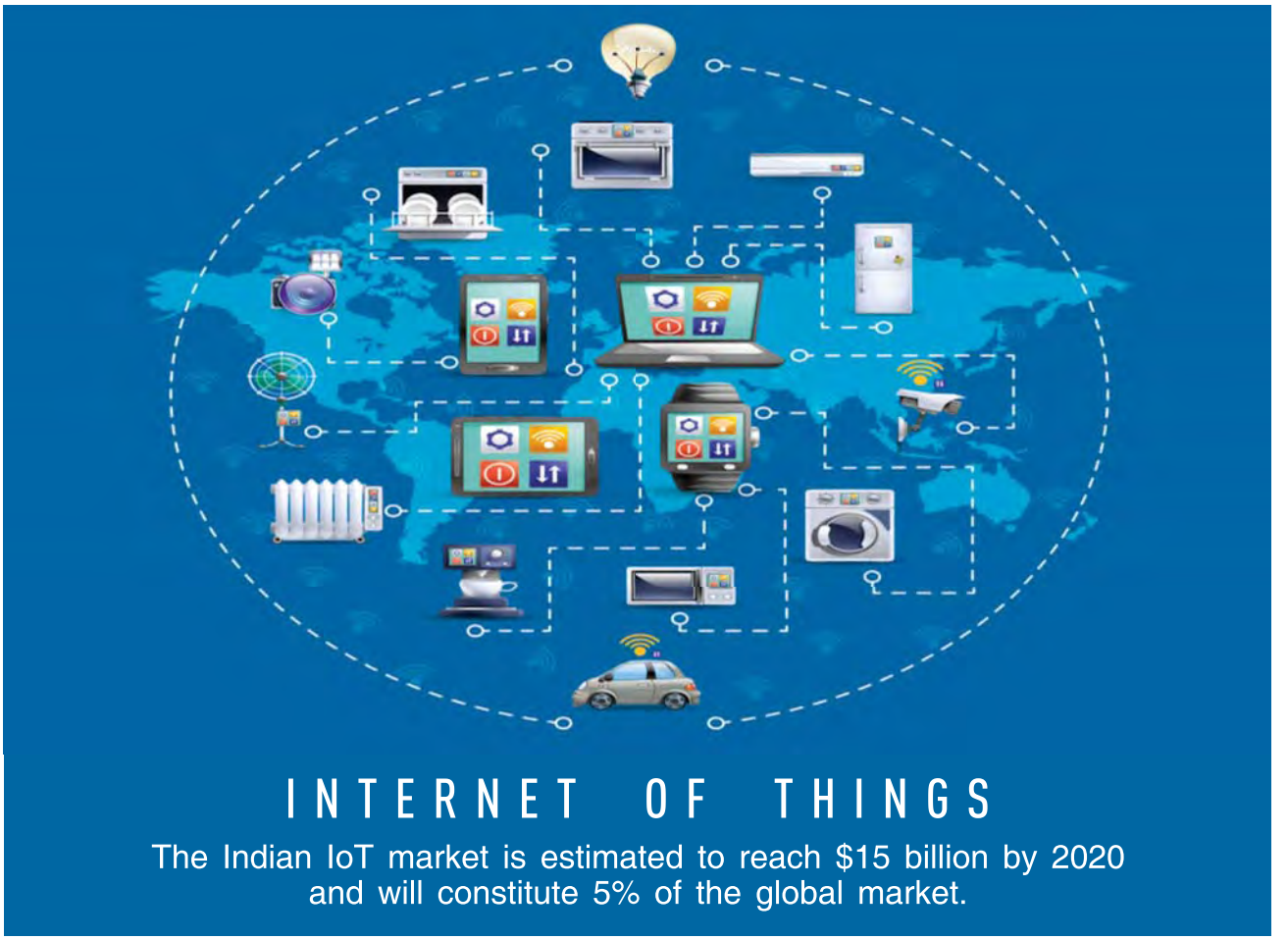
The landmark NDCP (National Data Protection Policy) released earlier this year is also an essential catalyst in prioritising the right breeding grounds to receive IoT technology. The policy aligns all digital communication stakeholders, and introduces a 'fibre-first' policy for greater fibre connectivity. This supports 5G technology that IoT will rely on. The amount of fibre in India is one-fifteenth that of the United States and one-tenth that of China and 80% of towers in China are fibre-connected but the same is only 20% in India. Another NDCP goal is to increase the number of public Wi-Fi hotspots in the country. More hotspots will grow IoT use by consumers. India, currently at 35,000 hotspots, will need more than 8 million to meet demand.

The draft Data Protection Bill has provisions for data privacy such as the Right to Information but also proposes enforcement of data localisation. Some entities feel this leans towards protectionism which could affect free flow of data across borders required for business and personal transactions. The draft bill advocates an overseeing committee but does not specify when and how this committee may access the personal data of Indian citizens.

Can we, as a nation, incorporate IoT-related measures that have been successful globally?

The EU's GDPR (General Data Protection Regulation) requires 'privacy by design' to be a core element of every step in the design of products and services. All IoT manufacturers can follow these guidelines to ensure that protecting privacy takes centre stage and is not added as an afterthought. Manufacturers can add a layered approach to data access and limit access to sensitive data. Devices must be upgraded regularly and tested for vulnerabilities.

Digital certificates and publicly key infrastructure (PKI) need to be incorporated to identify devices. Investing in sophisticated anti-breach software and security measures will improve data privacy upfront. This is advisable, rather than waiting for a breach and closing the metaphorical stable door after the horse has fled. Manufacturers can follow guidelines set by the Internet Society's Online Trust Alliance (OTA) IoT Trust Framework.



INTERNET OF THINGS

The Indian IoT market is estimated to reach $15 billion by 2020 and will constitute 5% of the global market.

With greater data privacy measures, Indians can enjoy the benefits of IoT just like several of our global counterparts. The US has almost 3,000 IoT-related businesses for an estimated value of $613 billion. Sweden is the world's most cashless society with less than 20% of financial transactions conducted through cash. Thanks to this forward-thinking strategy, the Swedes experience greater convenience and higher national security. The busy Shibuya station in Japan has over a million individuals passing through it per day. More than 60 bluetooth devices now connect to commuter smartphones through an app and direct traffic efficiently.

South Korean businesses saw revenues grow 23.4% to 7 billion won thanks to their government's investment in IoT technology early on. The residents of the smart city of Daegu, with a population of 2.5 million, reap the benefits of smart LED streetlamps, crosswalks, CCTVs for security, and intelligent parking. Gochang city reduced water costs by almost 20% in one year through smart IoT water metre installations. Estonians in Europe are members of an approximately 100% digitised society. Their government successfully moved most services onto a single, online platform and increased efficiencies.

It is high-time India joins the ranks of these nations in leveraging advanced IoT technology. We can control rising pollution levels. Healthcare can be more accessible and timely medical interventions can be made more likely. April 28th last year was a historic day in the development journey of India when the last village, Leisang in Manipur, was electrified. With smart IoT technology, we can bring greater connectivity to each household. The Indian government can realise the dreams outlined in the 'Make in India' and 'Digital India' missions through sophisticated IoT technology. As the world turns towards greater connectivity and technological advancements, IoT is here to stay. It is up to us to read the signs, drive progress and embrace this change for a vastly better India without losing focus on data privacy.

Research inputs by Chandana Bala

Author is honorary fellow, IET (London) and president, Broadband India Forum. Views are personal

5 million preventable deaths occur every year

Helpline

1800-11-0456

Reach out to us before you are one of them

Suresh Prabhu

Minister of Commerce & Industry and Civil Aviation

Modernizing Existing Industries

"We cannot rely on old industries alone.The term Industrial Revolution 4.0 is synonymous with smart manufacturing and it encompasses cyber-physical systems, Internet of Things, robotics, artificial intelligence, cloud computing and cognitive computing."

Edited excerpts:

Q How do you see the Indian economy performing?

To begin with, you have to look at the Indian economy from two perspectives. One is the fundamentals of the economy. Then there is the psychological factor that influences the economy. The economy is driven by people and people are driven by psychology. So psychology is as important as the fundamentals and psychology can change the fundamentals.

So, if you take both, the fundamentals of Indian economy are stronger and getting stronger every day. Savings rate is improving and the investment rate is growing too. We are also seeing improved exports and beginning of good activity in manufacturing. Services, too, are growing well. This is one part. Then there is the external sector, which is also looking better.

The second part is the psychological part. If you go by business confidence, it has, for the first time, improved in a significant way. If you go by the PMI (Purchasing Managers' Index) for manufacturing and services, it has improved too. And psychology, as I said, influences decision-making on real economy. So, we should look at better days.

Q The PM has laid a lot of stress on Make In India. How is it progressing?

The Make In India programme is an important component of not just make in India, but also the making of India. That's because the GDP can't be sustainable if manufacturing doesn't grow in good numbers.

We had a big manufacturing summit in Mumbai in which we asked the companies and industrialists who have been manufacturing for decades to make a plan that would make us a $5-trillion economy by 2026-27; and $1 trillion must come from manufacturing. We are now identifying sector by sector, for instance, how much must come from steel, pharmaceuticals, cement, chemicals and others. This is about modernising existing industries, scaling them up to a level where they can contribute to 20 percent of the GDP.

The second part is new industries. We cannot rely on these old industries alone. So Make In India must focus on industries that are new born today. We are trying to find out those industries and work on them as it's the new industries that will drive the growth of tomorrow. If you look at it, the company that will reach the $1-trillion market cap is a company that wasn't listed 20 years ago. There are companies that are listed for 100-plus years and they will never reach that mark.

Q Your ministry is looking at a new industrial policy. Can you tell us what that will look to do?

This policy will look into deregulation, new manufacturing facilities, industrial corridors, and specific products where manufacturing can happen on a large scale.

The new industrial policy, which will be released soon, will focus on modernising existing industries, besides pushing for frontier technologies like robotics and artificial intelligence.

Industries must come forward to respond on the changes which would come up on account of Industrial Revolution 4.0. The term Industrial Revolution 4.0 is synonymous with smart manufacturing and it encompasses cyber-physical systems, Internet of Things, robotics, artificial intelligence, cloud computing and cognitive computing.

Q But manufacturing across the world has been affected by Artificial Intelligence and automation. In that regard, how do you see the future of manufacturing in India?

There is no conflict in that. Manufacturing has changed over the last hundreds of years. What is important is that the manufacturing we will do tomorrow is relevant to the times. If you scale up the level of manufacturing, its capacity and propensity to create that many jobs in the old manufacturing sectors may not be as high as the new ones, but doesn't mean jobs won't be created. We will go into new industries and the modernisation of industries, which will create jobs. These new technologies may have some implications on employment generation in one sector, but it would create huge job opportunities in several other areas It is a misconception that automation doesn't create jobs.

Q How do you think 2018 is likely to shape up for India?

The Indian economy is doing far better than many other world economies. All Indians feel that we should do better. That shows that Indians have far more expectations from themselves; this will propel the economy. Business confidence and fundamentals are improving, and structural reforms are taking place to change the trajectory of growth.

"DIGITAL INDIA Has Become A Mass Movement In 4 Years"

Ravi Shankar Prasad

Union Minister of Electronics & Information Technology

Edited excerpts:

Q What have been the biggest achievements of this government in the digital technology sector over the last four years?

Digital India has become a mass movement touching the life of common and poor people. Four years down the line, common service centre movement has become big. From 23,000 common service centres in 2014, there are 2.91 lakh now. Apart from providing digital delivery of services, they have also created employment for 10 lakh people and have created entrepreneurship.

Q Bringing technology to rural areas of the country was one of the promises of this government. Apart from common service centres, where else have efforts been made?

Eighty-nine business processing and outsourcing units (BPOs) in 27 states of India in far-flung areas like Imphal, Kohima, Guwahati, Patna, Muzaffarpur, Bareily, Kanpur, Bhiwandi have been set up in the first phase of the rural BPO scheme. In the next lot, places like Ghazipur, Dewaria, Jahanabad and Gaya are going to be covered.

Q How much will the digital economy grow in the next five years?

We expect India's digital economy to achieve $1 trillion in the next five to seven years. This can be achieved easily. In fact, India's digital economy has the potential to grow to $2 trillion besides creating 40-70 lakh jobs in employment over this period. Government programmes such as Make in India, Skill India, Start-up India and Smart Cities will help reach the targets, and sectors such as IT and IT-enabled services, electronic manufacturing, e-commerce, digital payments and cyber security will be crucial in reaching these targets.

Q How will you achieve this?

It is achievable because the communication industry stands at $150 billion, IT and IT-enabled services stand up to $50 billion, both totalling to $300 billion. Electronic manufacturing in India is worth $100 billion, e-commerce $35 billion. Without including digital payments, the entire digital economy currently has a worth of more than $400 billion. Digital payments will become a $500 billion economy by 2020.

Q How have you improved governance through digital India?

India must come up with technology which is affordable, inclusive and developmental. We have done that through the Prime Minister's Jan Dhan-Yojana programme. For example, we created 28 crore Jan Dhan accounts of the poor that link to Aadhaar. Today, we have 68 crore bank accounts linked with Aadhaar. We have directly started sending subsidies — gas, ration, MNREGA — to bank accounts. Through this, we have saved about Rs 57,000 crore, which used to be pocketed by the middleman. In the Modi government, Rs 100 is being sent and Rs 100 is reaching the villages. Digital governance is good governance, digital delivery is faster delivery.

Q There have been concerns over websites publishing Aadhaar data. How are you addressing that?

Aadhaar as a platform is completely safe, secure and respects the privacy of all Indians. That is entirely inbuilt in the Aadhaar Act passed by the Parliament. About 113 crore Indians have Aadhaar and 99 per cent of the adult population of India is on Aadhaar. There is also a robust mechanism under sections 29,30,31 of the law where nobody can share their biometrics for unauthorised use, with due regard to privacy and data concerns. Anybody who tinkers with it will land in jail.

Q A key component of India's digital economy dream is domestic mobile phone market. How much has this grown?

India has come up well in the domestic mobile phone market. Manufacturing of mobile phones which was only six crore units in 2014-15 has reached an estimated 22 crore in 2016-17. In terms of value, there has been 183 per cent jump. In 2014-15,

mobile phones worth Rs 19,000 crore were made in India and today an estimated Rs 90,000 crore in 2016-17. About 72 new mobile manufacturing units have come up which has created one lakh new direct jobs and over three lakh indirect jobs.

Q Under your electronic manufacturing policy, it seems only mobile manufacturing has gained momentum?

Not true. There are various other schemes which are going on under our ministry such as MSIPs (Modified Special Incentive Package Scheme) and electronics manufacturing clusters. Under MSIPs, we are offering financial incentives to attract investments. About 269 investment proposals worth Rs 1,56,729 crore (till April 2017) have been received under MSPIs compared to only Rs11,198 crore in May 2014.

Q Are there any areas where more could have been done in the last four years?

In four years, the progress is remarkable. I have to accelerate its speed more in the areas like digital health, digital literacy and delivery of digital services. We have also seen enormous success of Aadhaar as part of the JAM (Jan Dhan-Mobile-Aadhaar) trinity. As of date, there are 30 crore Jan Dhan accounts, 120 crore Aadhaar and 121 crore mobile phones in the country. We have saved over Rs 90,000 crore through direct benefit transfer. Fictitious claimants and middle-men are now out. Four

"We owe India a digital revolution"

– Ravi Shankar Prasad

years have shown poor people getting empowered through technological developments such as e-hospital, soil health cards, e-scholarships, Jeevan Praman Scheme, e-NAM. All of this technology is homegrown.

Q Data can be misused and we've recently seen how. With growing digitalisation, this fear of misuse is also increasing.

We are very proud of the Digital India initiative. Of our 1.3 billion people, 1.21 bn have mobile phones, 1.2 bn have Aadhaar cards, 500 million are internet users and India is emerging as a big digital market, with growth in e-commerce and digital payments. Growth of home-grown technologies is the marvel of Digital India. The government has saved Rs 830 bn by using digital means. In any digital platform, data is important. Facebook has its biggest footprint in India; then, we have Twitter, LinkedIn and WhatsApp. Our government is committed on data safety and security.

Q Data is growing but it should be protected. What are the safeguards for ensuring this?

When you talk of data protection, one concept should be clear. It's about data availability, data utility, data innovation, data anonymity and data privacy. The core data of an Indian or any individual must be respected and protected. Medical records, income, personal or family record, bank account and sexual preferences are personal things and should be protected.

Q You say a bank account is private but when linked with Aadhaar, the details can be made public.

When I talk of a bank account, I talk of the account details. Bank accounts are being linked with Aadhaar because of changes in rules under the Prevention of Money Laundering Act. However, bank details like amount and other things cannot be made known to others.

Q The government is working on framing a data protection law. When could we expect this?

The B N Srikrishna committee is working on the report and it will be a comprehensive law. We have made the Aadhaar Act. UPA's (the earlier government's) Aadhaar was without a law. Modiji's Aadhaar is with a law, with due provision for safety and security. Data is important and any digital connect creates some sort of data. We have to accept this truth. Data is important for a study or information but it should be anonymous. We wish India becomes a centre for data analysis and our young human resource will do it. However, data should not be misused and those who misuse, tough action should be taken against them.

Q What has the government done to safeguard data, particularly on social media?

The IT ministry has conveyed to all social media platforms that they should not become platforms for abuse, hatred, crime and terrorism. A senior Twitter official met me recently and I told him Twitter should not be used to troll or shower abuse during election campaigns. All social media companies are welcome to do business in this vast country of 1.3 bn people but must keep in mind the sensitivity, amity and understanding of the people. My government fully respects freedom of press, freedom of speech and also freedom of social discourse on social media. But, under the Constitution, the right of speech is also subject to reasonable restrictions.

Q Under what rules could action be taken against companies found to be misusing data?

A sovereign country has the trust of the people. There is enough existing substance of power under the IT Act about sensitive data and information. There is also the Indian penal code.

Q You've served a notice to Facebook but when could we expect officials of the company to be summoned for questioning?

I will await the nature of their response for further follow-up action.

Q Players such as WhatsApp are being used to spread fake news. How are you tackling that?

India is becoming a big centre of WhatsApp and I am happy that it is being used in every area but I also worry about its misuse. We need to make a collective decision, without compromising the freedom of speech. OTT (the term for entities such as WhatsApp, a provider of audio, video, and other media services directly to the consumer over the internet, bypassing traditional providers such as broadcast or cable firms) apps are not outside the jurisdiction of Telecom Regulatory Authority of India (Trai). Although norms regarding these apps are not there, they are subject to Trai regulations. The operators of WhatsApp must also be vigilant and ensure their platform is not prone to abuse. Constructive engagement of any data company is not wrong. If I am posting my message on Facebook to reach 50 lakh young people, what is wrong with that? However, influencing elections using unauthorised means on social media should not be at all allowed.

Q What action can the government take if someone misuses WhatsApp to spread fake news?

Any abuse of the WhatsApp platform is subject to all the stringent punishments under the IT Act and also the penal code. It has to be calibrated in a way that the data discourse and resultant digital development of India not be unnecessarily handicapped but it should also remain safe and secure.

HMD

DISPO VAN

THE TRUSTED BRAND PROMOTING PATIENT SAFETY

MADE IN INDIA, CURING PEOPLE AROUND THE GLOBE

Precision Engineered, Affordable & Easy to use.

www.hmdhealthcare.com • info@hmdhealthcare.com

AFTERWORD

Pyush Misra
Director,
Consumer Online Foundation

In our recent research on AI in customer experience, we found that that 45% of consumers are willing to delegate routine tasks to such a voice-enabled assistant. What's more, around one in two consumers (48%) found the idea of such an assistant exciting and 46% said it would improve the quality of their life.

Empathetic Intelligence: How Smart Voice Assistants Are Transforming The Way Brands Drive Consumer Convenience

AS A CONSUMER, what would you rather do: talk to a voice assistant, navigate your way through an app, or visit a physical store?

This is the question we asked 5,000 consumers in a research. The answer we received highlighted the fact that – consumers are embracing voice assistants today and many see a future where voice assistants will trump websites or physical stores.

Some key stats below:

- Over half (51%) are already users of voice assistants, largely via smartphones (81% use this mode).
- Three years from now, 40% say they would choose a voice assistant over a mobile app or website.

Starting with the movement of consumers from physical stores to online shopping a few years back, to the preference towards voice assistants for routine shopping tasks today, convenience is increasingly driving the way consumers make decisions.

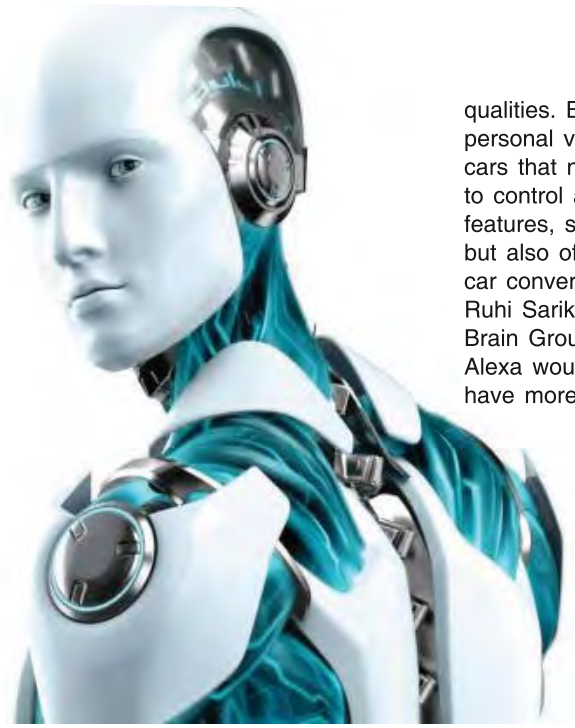
In today's attention economy, the consumer has plenty of choices. The onus lies on organizations to capture the limited attention of consumers and devise compelling customer experiences that build long-lasting relationships.

When we asked consumers why they prefer voice assistants over websites and apps, the top 3 drivers were:

1. It is more convenient
2. It allows me to multi-task and do things hands-free
3. It helps me automate my routine shopping tasks

And when we asked why they preferred using voice assistants instead of human assistants in a shop or call center, the top 3 results were:

1. It is faster
2. It is more convenient
3. It provides greater choice



Convenience is not limited to just shopping or routine activities. It is also about delegation. At its annual developer conference in May 2018, Google introduced Google Duplex, an AI system for real-world tasks that uses a natural language interface. The technology engages with humans over the phone in a conversational, human-like manner. In our recent research on AI in customer experience, we found that that 45% of consumers are willing to delegate routine tasks to such a voice-enabled assistant. What's more, around one in two consumers (48%) found the idea of such an assistant exciting and 46% said it would improve the quality of their life.

How will brands sustain an emotional link in a voice assistant future?

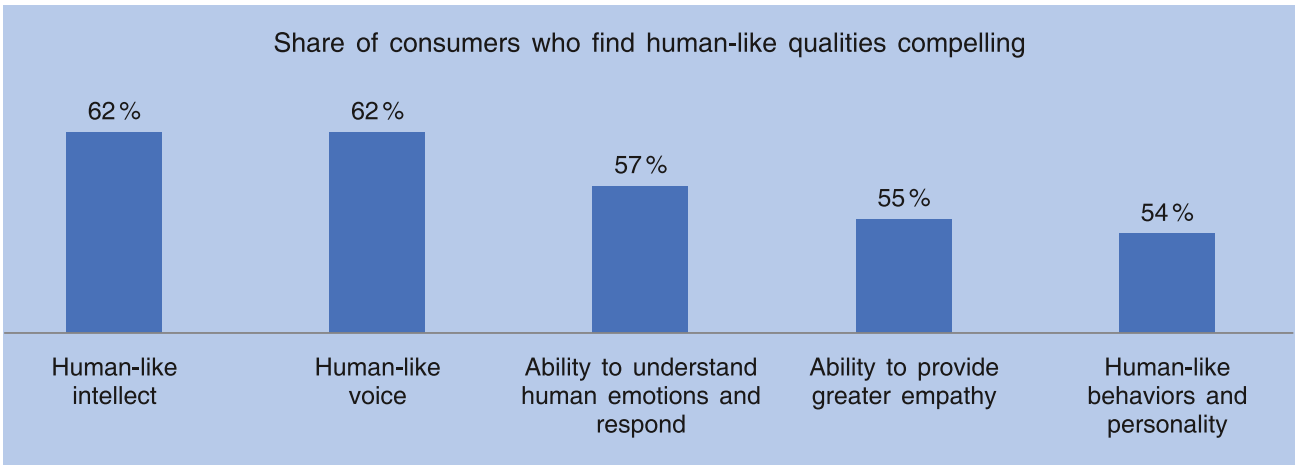
If they are to meet consumers' needs, organizations are going to have to keep pace with these fast-changing expectations. They also need to understand the full implications for their digital customer experience. For example, how will brands sustain their emotional connection with the end-consumer in a world where there are fewer direct interactions?

It is critical, thus, for convenience to not be delivered at the cost of empathy and an emotional connect with consumers. In 2017, it was found that emotions have the strongest impact on loyalty. We also found that the ability to connect on a human level is what drives long-term customer engagement and, ultimately, loyalty. When it comes to how smart technologies are used as part of the customer experience, human-like qualities, therefore, become critical. In our AI in Customer experience research, we found human-like voice and intellect as the top two compelling factors in AI-enabled interactions with organizations (see Figure 1 below):

This is why some innovative companies are striving to meet the demand for voice assistant convenience married to human-like qualities. BMW has launched a personal voice assistant for its cars that not only allows drivers to control all the standard in-car features, such as climate control but also offers more casual in-car conversations.And Amazon's Ruhi Sarikaya, head of the Alexa Brain Group, announced that Alexa would soon be able to have more natural conversations, allowing this technology to understand and respond to follow up questions.

It is clear that conversational interfaces present brands with a unique opportunity to meet consumers' changing needs while retaining an emotional connection. Consumers are not interested in the technology or platform that brands deploy, rather the experiences they deliver. Organizations need to build the voice of their brand, where brand personality is maintained while delivering a seamless and personalized experience. As the uptake of voice assistants grows, and the technology advances, organizations must deploy effective strategies to tap into this potential.

Figure 1: Consumers prefer human-like qualities to make AI-based interactions more compelling



THE AWARE CONSUMER

An opportunity to SPEAKUP!

Join the Movement ...

Save upto 50% on subscription

Subscribe today!

{Save ₹3,600/- FOR 36 ISSUES}

India's more credible consumer monthly from renowned Consumer Activist Bejon Kumar Misra

Please accept my subscription of **THE AWARE CONSUMER**

NAME _____

ADDRESS _____

PH. NO. _____ E-MAIL _____

PAYMENT ☐ CASH ☐ CHEQUE CHEQUE/DD NO. _____

DRAWN ON _____

DATE _____ SIGNATURE _____

No. of Issues	News Stand Price	Discount	You Pay	You Save
12	₹ 2,400/-	20%	₹ 1,920/-	₹ 480/-
24	₹ 4,800/-	30%	₹ 3,360/-	₹ 1,440/-
36	₹ 7,200/-	50%	₹ 3,600/-	₹ 3,600/-

Cheque / DDs should be drawn in favour of **BEJON KUMAR MISRA**

Send your subscription to: The AWARE CONSUMER, F-9, 2nd Floor, Kailash Colony, New Delhi-110048

Contact: 9811044424 • +91-11-40537140 • E-mail: bejonmisra@gmail.com

THE AWARE CONSUMER
STATE AWARDS

4TH EDITION

THE AWARE CONSUMER STATE AWARDS

on the occasion of

NATIONAL CONSUMER DAY

24 December 2018 • NEW DELHI

- **THE MOST CONSUMER FRIENDLY STATE – HIMACHAL PRADESH**
- **THE 2nd MOST CONSUMER FRIENDLY STATE – GOA**
- **THE 3rd MOST CONSUMER FRIENDLY STATE – ANDHRA PRADESH**
- **THE 4th MOST CONSUMER FRIENDLY STATE – KARNATAKA**
- **THE 5th MOST CONSUMER FRIENDLY STATE – ANDAMAN AND NICOBAR ISLANDS**
- **THE STATE WITH BEST DIGITAL PRESENCE – KERALA**
- **THE STATE WITH BEST DIGITAL PRESENCE – MAHARASHTRA**
- **THE STATE WITH HIGHEST CONSUMER COMPLAINT REDRESS – CHANDIGARH**
- **THE STATE WITH 2nd HIGHEST CONSUMER COMPLAINT REDRESS – TRIPURA**
- **THE MOST IMPROVED STATE – MANIPUR**

THE AWARE CONSUMER

QCI

PROGRESS HARMONY DEVELOPMENT PHD CHAMBER Estd. - 1905

To access the full Report of the event visit **www.theawareconsumer.in**

Digital Marketing Trends That Are Changing The Way We Market To Consumers

– *Atanu Shaw*

THE WORLD IS changing, and technology is taking the lead. Today, everything is going digital -- entertainment, health, real estate, banking and even currencies. This is, however, understandable. In North America alone, 89% of the population is online (subscription required).

With everything turning to digital, it means companies are also jumping online to market their businesses. And to survive the challenges of digital marketing, brands need to keep up with the latest trends. Successfully reaching one's target audience is no longer just putting out TV and print ads. These days, social media is the new arena of digital marketers, as 3.3 billion people are active social media users.

Notably, according to January 2018 data, 24% of the 5,700 global marketers who were surveyed revealed that social media has been an important part of their marketing for the past five years.

To keep up with the ever-changing scene, digital marketing experts need to stay in step with the evolving tech trends. Social media marketing companies work

tirelessly to research consumers and what makes them engage with brands. We try to find the best online solutions that will cater to our clients' end-users' queries in the easiest and most cost-efficient way possible -- be it by developing new technology or adapting to trends.

After much research, here are the leading digital marketing trends that are paving the way in 2018.

1. Interactive Chatbots

Chatbots have been around for some time now. The technology, which combines the use of text, voice and messaging to converse directly with consumers, has been used longer than virtual reality. But this year, it's taking the spotlight.

According to a 2017 report by Grand View Research, the global chatbot market is estimated to see a compound annual growth rate of 24.3% and is projected to reach $1.25 billion by 2025. In 2017, LivePerson conducted a survey of 5,000 consumers based in six countries and found that 67% of those surveyed are using chatbots for customer support. Furthermore, 38% had positive feedback, and only 11% registered negative reactions to the technology.

Messaging applications such as Facebook Messenger and WhatsApp also make use of messenger bots that are customized to push out products and services. They do this not only by promoting the brands, but also providing the potential user a personalized customer service experience.

The main reason why this technology is so successful is likely that it answers the consumers' need for information quickly and accurately. Chatbots can also collect data about their users, which feeds into improving interaction with them.

Of course, much like any other technology, there are a few things to note before adopting it. Marketers should consider where to use chatbots. For example, businesses with greater Facebook engagement may want to incorporate a chatbot in their Facebook Messenger; those who have more website traffic may benefit more from website chatbots.

Nonetheless, the tech not only provides a more efficient and responsive way to deal with customers; it is also more cost-effective than hiring customer relations staff.

2. Voice Search

As more and more people are on the go, the use of voice search and voice commands is increasing. Voice assistants are empowering mobile users to access information online and do certain tasks like never before. In the U.S. alone, the use of voice assistants is expected to grow by 128.9% in 2018, compared to 2017. That's a total of 35.6 million Americans using the service at least once a month.

While the growth is positive, it is a big challenge for businesses as well. Unlike the usual online searches with pages upon pages of results, voice searches will only give the top, most related answer to a query. Businesses want to be that one result that matches a user's voice query.

What does this mean for digital marketers? It means optimizing content to suit the requirements of voice searches. Publish content that solves or answers consumers' queries. It's also important to use natural conversational language, as well as longer phrases or full sentences as keywords. This not only helps the end-user but also makes the content voice-search-friendly.

3. Integrating AI And Blockchain Technologies

Blockchain technology is already disrupting the way the world views finance and financial systems. Its power is not limited to these sectors, however. In recent years, it has already expanded to digital marketing.

Technology has allowed marketers to track where their ads are placed and ensure that real consumers, rather than automated bots, are clicking on their ads. This makes customer engagement data more reliable and makes sure brands' marketing assets are not being put to waste.

Consumers can also benefit from the transparent nature of blockchain technology, as it gives them more control over how their personal data should be used by advertisers. When consumer trust increases, the likelihood of them sharing personal information also surges. This helps marketers and companies to know them better.

There are a few game-changing services that can help marketers effectively track marketing efforts through blockchain, making sure that every penny is being put where it's supposed to go. While this would mean additional expenses, the return on investment makes it worth the extra dollars by making sure every ad reaches the target audience.

4. Influencer Marketing

In today's world, where social media is ubiquitous, people tend to gravitate toward experiences that are authentic and real. And potential customers are more likely to believe a real person over an advertisement about how good a certain product or brand is. This is where influencers come in.

While influencer marketing can be very effective, it may also be costly. To get the most out of a business's marketing budget, marketers should choose their influencers carefully and make sure the ambassadors they use cater to and reach the right consumers. Using an effective hashtag that people can easily remember and adopt will further help the campaign.

For digital marketers to become more effective, regularly assessing and evaluating strategies should be commonplace. Taking note of the latest digital marketing technologies and trends will be the driving force for success.

The 15 Best Smart Home Products to Buy in 2019

Make your home more efficient with these smart products

by Tim Boyle and Jay Schneider Updated January 10, 2019

The Rundown

- **Best Smart Display for the Kitchen:** Lenovo 10" at Best Buy, "Integrate it into your kitchen, where you can have it help build your shopping list."

- **Best Smart Display with Google Assistant:** Google Home Hub, "Bringing you all the perks of an Amazon Echo at a reasonable price."

- **Best Smart Home Assistant:** Amazon Echo Plus 2G at Amazon,"Access Alexa voice assistance to run web searches, ask questions."

- **Best Budget Assistant:** Amazon Echo Input at Amazon, "Connects to your Wi-Fi and plugs into an existing speaker system to give that speaker Alexa functionalities."

- **Best Smart Display with Alexa:** Echo Show 2G at Amazon, "Dolby-tuned speakers give you solid stereo imaging and nice, detailed sound."

- **Best Smart Display for Music:** JBL Link View on JBL.com, "Can play your media through its speakers without the need for another audio device."

- **Best Smart DVR:** Fire TV Recast at Amazon, "Puts live TV and recording features at your fingertips — all without an additional monthly fee."

- **Best Smart Home Security Camera:** Ring Stick-Up at Amazon, "Not only will this work via the app on your phone, but it will also work on a desktop computer."

- **Best Smart Home Security System:** Abode Essentials at Amazon, "Compatible with the major smart home systems so it can easily integrate."

- **Best Smart Thermostat:** Nest Learning at Amazon, "The Nest learns and adapts to your own personal habits and preferences."

- **Best Smart Light System:** Philips Hue at Amazon, "Boasts a highly intuitive user experience with a simple app and easy-to-install component parts."

- **Best Smart Plug:** Amazon Smart Plug at Amazon, "You can set automatic turn-on and turn-off times for things like table lamps, fans, or even small appliances."

- **Best Smart Vacuum:** iRobot Roomba i7+ at Best Buy, "Even if it vacuums every day, you'll only need to empty the bag once a month."

- **Runner-Up, Best Smart Thermostat:** Ecobee3 at Amazon, "Ecobee expects owners to be able to save an average 23 percent on monthly heating and cooling costs."

- **Best Smart Smoke/Carbon Monoxide Detector:** Nest Protect at Amazon, "Sends a message to your phone if the alarm sounds or the batteries are low."

SMART CITY

A **SMART CITY** is an urban area that uses different types of electronic data collection sensors to supply information which is used to manage assets and resources efficiently. This includes data collected from citizens, devices, and assets that is processed and analyzed to monitor and manage traffic and transportation systems, power plants, water supply networks, waste management, law enforcement, information systems, schools, libraries, hospitals, and other community services.The smart city concept integrates information and communication technology (ICT), and various physical devices connected to the network (the Internet of things or IoT) to optimize the efficiency of city operations and services and connect to citizens.[3][4] Smart city technology allows city officials to interact directly with both community and city infrastructure and to monitor what is happening in the city and how the city is evolving.

Demystifying The Current State Of India's Ambitious Smart City Mission

THE CONVERSION OF a large, crowded and unplanned city in India to a Smart City is currently an impossible scenario to imagine. Taking a smaller town, not overrun by people, vehicles and multiple layers of red tape or 'babudom', and converting it into an ideal, intelligent, self-sufficient and secure ecosystem is still workable.

However, In India, the progress towards achieving the goal of 100 smart cities by 2020 has clearly become sluggish owing to inaction, a lack of understanding, a dearth of technical training & skill building, and most of all the non existent security framework.

Essentially, 'smart cities' exploit networks that already exist but are still hidden, whose potentiality is unexploited. There are many possible synergies that can be activated bringing together businesses, cities, research communities, and civil societies.

While there is big talk of technologies like smart lighting, smart waste management, better surveillance, smart traffic management, and such, for now, the common Indian folk are yet to witness the wonders of living in a smart city in their daily lives. In the real world, traffic jams in large metro are still killing us softly, electricity or the lack of it is still an issue unresolved with every changing government, safety - physical or cyber - is a big joke, people as well as civic bodies use the natural environment as their personal dumping ground and the internet is still a fairly new concept in the country after 35 years of its existence.

According to a report released by the Minister of Urban and Housing Affairs, Mr. Hardeep Singh Puri, 148 projects have been completed till date under India's Smart Cities Mission. Besides this, 407 projects have started work, and another 237 projects are in the tendering stage. So while things have progressed slowly until now, there are very encouraging signs that India's Smart City Mission will be successful. Further 82 out of 99 cities now have functional Special Purpose Vehicles, who monitor, assess and implement their cities smart city projects. Furthermore, the state and central governments have created an efficient system for the flow of money, so that SPVs are not hindered by financial problems. India may not finish transforming 100 cities into smart cities by 2020, but the mission is very much on track – providing smart technology to 100 cities by 2020.

ROADBLOCKS

Having been used to a relationship of doling out grants to cities and its citizens the administration has grown too accustomed to not being accountable and not having to be questioned on quality of delivery. They now have to come up with sustainable solutions and be accountable for them. This requires a change in mindset. Secondly, even if the mind-set underwent a change, capacity building remains a huge hurdle. Finally, legacy of old technologies and systems further complicates the ability in making valuable offerings. Theseare the biggest roadblocks to developing smart cities in India. Finance is another huge obstacle especially in light of the focus on public-private partnership (PPP) model to fund smart cities projects.

For companies such as HPE, Intel and Cisco who are leaders in Smart City technology around the world, it is hard to imagine that they would invest so many millions without having a clear plan for viability and financial benefit. Firstly, investing so heavily in smart cities gives these companies an opportunity to create and operate these cities of the future in a way that they see fit, thus making their imprint on the future which by itself is a tremendous incentive. Furthermore, they have the opportunity to leverage their platform and network in order to create new sources of revenues in areas such as advertising, data analytics and subscriptions. Lastly, by displaying leadership, and managing the entire implementation, operations and partner ecosystem of the smart city initiative, large companies are involved in decision making at the governmental level, thus giving them a voice in more issues that can benefit all parties

The biggest hurdle in controlling cities through command and control centers is the training aspect of those set to control it. CCCs, when implemented fully, will do nothing but improve the accessibility of services and government to citizens. It will enhance the ability of officials to respond fast to situations, by leveraging good quality data and information, and ensure the best for people. Consequentially, this requires an intensive training process for those who will work in Central Command Centers. There is a need to ensure a rigid training program that would prepare city officials to act quickly, and prepare them to react to emergencies calmly. This may even require foreign assistance from cities such as Rio De Janeiro who have successfully set up CCCs, and run them efficiently.

REGULATORY FRAMEWORK

The current regulatory framework in place for smart cities in India can definitely be made stronger. Currently, the Information Technology Act governs the scope of internet activity in India. However, the introduction of smart cities has created a surge in “Big Data”, i.e. enormous sets of unstructured data analysed computationally to understand patterns relating to human behaviour. This poses new challenges regarding privacy and personal information that are currently not defined under the act, which can leave smart cities vulnerable. Furthermore, the National Cyber Security Policy, and the Geospatial Information Regulation Act also fall short of properly protecting data and privacy under smart cities. In time to come, it may be essential to examine the feasibility of developing a comprehensive law on cyber security, privacy, data protection and standardization of equipment. India is currently doing its best to safeguard its citizens and their data, but with the government's ambitious Smart Cities Mission, and the quick progress towards a new digital age, there is a new framework needed to account for smart cities.

The Government of India launched its Digital India campaign and its Smart Cities Mission in 2015, after which improvements in online infrastructure are slowly being carried out. In a country such as big as India, which is still developing on a cultural and economic front, there were basic changes that were needed to even provide the common man everyday easy access to the internet. However, albeit slowly, the government has made technology a forefront in everyone's life. IoT is a relatively new and modern concept in India, where we are still trying to deliver stable electricity and connectivity to every corner. Thus, IoT is still an alien concept to the country. Applications of technology in resolving daily city life issues are a good start as parking, public safety, lighting projects are introducing this concept to citizens and officials. However, through public awareness conferences and seminars held by the government, the IoT is slowly being discovered and put to use in everyday applications.

IoT technology stretches to all sorts of appliances from household objects to industrial ones, with new applications being developed every day. In India, these advances are taking shape very rapidly, with Deloitte projecting that by

What does ‘smart city’ mean?

“A smart city is a place where the traditional networks and services are made more efficient with the use of digital and telecommunication technologies, for the benefit of its inhabitants and businesses.

2020, there will be 1.9 billion IoT units in the country and that the market value of this sector will hit $9 billion. With the strong focus on smart cities now, tier 2 and 3 cities are also in line to implement IoT at a faster rate than other countries. While currently, these projections may be limited to smaller household objects and appliances, but by 2025 it will extend to full industrial use, and for applications like smart waste management and smart homes.

There are a few barriers that would impede the deployment of an automated energy management system in India. Apart from the widespread 'kundi' connections which would take a huge amount of investment to take down, there are other challenges to this problem. An automated energy management system would result in an increased load on the electric grid, and the ever-changing weather in India would also increase its unpredictability due to changes in cloud cover and wind speed, complicating the scheduling of power generation. Furthermore, in the presence of a large number of sensors, enormous amount of data is generated. Data may have issues like missing values, corrupted values and inconsistencies. These can further complicate the process of energy management and also introduce other problems, such as privacy, which is already an unstable issue in the country. Even local heating and cooling systems commonly found in EU countries may be too expensive to implement in India.

Some of the leaders of Smart City development worldwide are Hewlett Packard, IBM, and Cisco. In India itself, HPE has managed to provide the best features for managing cities effectively and in a cost-effective manner. Bhopal, Kakinada and Pune are just some of the cities that have been positively impacted by the work of these IT giants. Some cities now have an efficient provision for integrated and scalable solutions, as well as an optimum use of resources like sharable infrastructure. These companies have also brought Indian cities a single interface for the implementation of multiple solutions, integrated and scalable infrastructure solutions, and made it easier to execute, coordinate and monitor various projects. For example, in Pune the implementation of a CCC in public transportation has increased the modal sharing of public transport throughout the city, increased convenience for citizens, and increased the control of bus movement, which helps Pune's transportation provider to manage its own fleet and the operation of its running buses in the most effective manner.

As per the power ministry's strategy to implement solutions like smart meters and smart home energy management, it predicts that such technologies would become commonplace in India only by 2027. The plan is to install 'advanced metering infrastructure' in phases, with those consuming 500kWh or more by 2018, those consuming over 200 units by 2020 and then 2027 countrywide. This is due to such smart solutions needing good data connectivity not only in large cities as well as in remote and rural areas. India is still in the process of distributing good data connectivity, making the power ministry's predictions logical. Furthermore, there are more challenges that impede smart energy management solutions in India. These include the need to setup a communication between the technology and control centre which is proven to be a difficulty due to connectivity problems in the country, as well as the intense personnel training required to manage such a large operation.

City-wide connectivity allows much more room for a single security vulnerability to wreak havoc on the residents and governments that have adopted smart cities technologies. As more cities adopt more Smart City technology to replace or upgrade existing infrastructure, the risks they carry will only grow and compound. Thus, there is a need to make smart technology cyber-safe. This means that developers in India need to work with one another in tandem, to make sure there are no lapses in online security. Smart cities can also implement predictive cybersecurity analytics, which would prevent data breaches and continuously find gaps in security infrastructure to improve them before they can be exploited by outside attackers. Responsible citizens who are trained to make smart lifestyle choices, keep their own data secure, and contribute to public awareness campaigns can also go a long way towards pre-empting major cybersecurity threats.

Forces That Will Shape The Future

What Key Questions Do They Raise?

SMART CONSUMERS GET PERSONAL

- Consumers are increasingly shopping online, when they want, using a variety of devices – and requesting choice in delivery services
- Consumers will pay more for services such as faster delivery, and want to track goods all the way
- The personal supply chain model has created new opportunities – but many businesses are yet to adapt
- Retail and other business-to-consumer industries need to invest in the right combination of technologies

WE BELIEVE CONSUMER-FACING industries will change beyond recognition over the next 10 years. We have identified eight hypotheses about the forces that will drive this change and transform the way companies create and capture value.

These are the kind of disruptive paradigm shifts that characterize the transformative age we are living in. Each has the potential to suddenly take an exponential growth path, where change becomes bewilderingly fast and powerfully disruptive.

Underpinning our hypotheses is the emergence of what we call "The Smart Consumer." People are already analyzing their personal data to improve their lives and become better versions of themselves. Half of all developed-country employees use a wearable device or other technology to track their fitness and sleep patterns.As the technology evolves and data becomes ubiquitous, The Smart Consumer will fine-tune everything they do.

Artificial intelligence will nudge and guide them through this process of life-enhancement. Their super-intelligent AI "companion" will be at their command and with them everywhere. AI will help The Smart Consumer to optimize everything – from what they eat and how they feel, to how they spend their social time and progress their careers. It will even help them manage their personal relationships.

Companies that want to serve these future consumers and build profitable relationships with them will have to reinvent themselves.

1. WHEN BOTS DO THE BUYING, WHERE'S THE VALUE IN SHOPPING?

Most of the purchases we make today require some element of conscious choice. But as AI bots, concierge services and smart-home systems become more intelligent, they'll complete many of these transactions for us.

Consumers will receive competitively priced and relevant products via technology-based platforms that serve as access points to new buying ecosystems. These platforms will use AI and machine-learning technologies to draw on vast quantities of data and predict or preempt customer behavior. This will disintermediate transactions, payments, fulfillment and brands.

Key question: What happens when buying becomes shopping?

Over time, consumer engagement will polarize. We'll become completely disengaged from most of the products and services we buy and super-engaged with a few.

In the majority, our personal technologies will evaluate what products or services we need, when we need them and where best to buy them – not just in terms of finding the right price, but also in terms of sourcing brands and suppliers that align with our values.

We'll trust these intermediary technologies to curate the right choices and purchases on our behalf. Today, 47% of consumers already say there are open to the idea of buying items through a chatbot. And almost half of US consumers say they are willing to share personal

information if it gets them a better deal.

As buying becomes more automated, it will become a very different activity from shopping, which will also evolve. We will actively "shop" for only a select few brands. These purchases will help us express and shape our identities and give us an amazing experience.

The majority of consumer products will become commoditized as a result, and the face of retail will change forever.

2. WILL YOU SELL PRODUCTS OR ACCESS TO LIFESTYLES?

With the rise of the gig economy, a more nomadic consumer base and the growth of mega-cities, future consumers will continue to move away from owning things. Instead, we will trust on-demand services to meet our needs – as they arise, and just in time. Businesses will need to reflect the new ways people live and work.

Today, companies like Spotify and Uber give us subscription or pay-to-use access to assets and experiences that past generations had to own. Consumers are getting used to this model and the convenience it gives them. They expect everything to be flexible and focused on their needs. The relationships we form with brands – and with one another – is changing.

Key question: What happens when lifestyles replace products?

In the future, this model will apply to a much wider range of products and services. Even the spaces we live and work in will morph to reflect the needs of the moment, with our homes becoming larger or smaller to reflect who's at home.

As we own fewer things and become less encumbered by place, we'll be able to move location and shift between new cities with ease. Patterns of global consumption will change as a result.

The United Nations predicts that by 2030, urban areas are projected to house 60% of people globally and one in every three people will live in cities.

3. WHEN HEALTH IS PASSIVELY MANAGED, HOW ACTIVE CAN BRANDS BE?

Today, it takes thought and conscious effort to live a healthy life. From following an exercise program to reading the nutritional labels on products to booking an appointment with the dentist, we need to actively take care of ourselves. The few health-care technologies that are available to us are relatively dumb.

In the future, once we establish a trusted relationship with providers to share our data, we'll be able to connect to a sophisticated infrastructure of technologies that actively and automatically monitor, improve and maintain our health and well-being.

We won't need to think about it, and we'll barely be aware of it.

Key question: What happens when Healthy is the default?

From an early age, children will have their future mental and physical health mapped out through detailed analysis of their genome. This map will update as they mature logging their nutritional needs and the exercises they undertake. The services and products they consume will adapt to their evolving health needs.

We'll eat meals that look and taste like steak, but are actually 3-D-printed plant proteins containing vitamins and nanomedicines designed specifically for our bodies. The US federal government is already spending $1.2b a year to fund nanotechnology research. In the future, “paradox products” that look like normal foods and drinks but fulfill invisible, beneficial functions will be common.

Our exercise needs, social activities, meal plans and preventative therapies will be integrated and personalized into every area of our lives, nudging us gently toward self-improvement – all part of a passive consumer experience supported by a smart, ever-evolving system.

4. WHEN DATA REVEALS THE IMPACT OF EVERY MEAL, HOW WILL YOU HELP CONSUMERS MAKE BETTER CHOICES?

Today, what and how we eat is steeped in complexity and shrouded by uncertainty. We don't really know where our food has come from or how it's made its way to the plate. Not so in the future. There will be a fundamental shift from “food fiction” to “food fact.”

What we consider to be a good meal will change, as blockchain technology facilitates a completely transparent food system. The environmental impact of each food choice we make will be clear. As a result, we'll eat far less meat and much more plant-based food.

We'll learn much more about nutrition, the human body and the personal impact of our dietary choices on our health and well-being and the environment. With reliable data about how our bodies are performing at any moment in time, we'll be able to eat and drink products that are personalized to satisfy our precise and unique dietary needs.

Key question: What happens when data determines what you eat?

Today, most of us have to choose between taste, convenience and wellness. For future consumers, this trade-off will disappear. We'll be able to eat and drink things that are great for our health, are quick and convenient, taste fantastic, and reflect our ethical values.

A recent global survey yielded that nearly 90% of consumers would be willing to pay a premium for products with added health and wellness benefits.

5. HOW WILL YOU MAKE YOUR TECHNOLOGY SO SMART IT'S INVISIBLE?

The technologies people use today have become more interactive and better integrated with daily life. But we're still aware that we're using them. In the future, we'll be far less aware of technology – many of the services or devices we rely on will become invisible.

A world where information, technologies and data are fully integrated will remove friction and add incredible value to consumers. With nearly 20 billion “connected things” expected to be in use by 2020, many of the technology interactions we experience today will melt away.

We'd never have to carry IDs, bank cards or door keys; every service we receive can be personalized and adapted to our specific context. This paradigm shift would have a massive impact.

One forecast suggests 10% of global GDP will be stored on blockchain by 2027.Costs for businesses, governments and other organizations could be radically lower, and new kinds of product or service would become possible. Companies would be able to optimize their supply chains in ways that are impossible today.

Key question: What happens when technology becomes invisible?

For this level of integration to happen – without vertical and total monopolies forming – different platforms would have to collaborate and exchange information with one another in a fraction of a second.

Automatic, negotiated interaction will need to be a highly intelligent and end-to-end process. The notion of competition will change radically. People will need to learn to trust an AI to make decisions on their behalf.

6. WHEN LIFE IS GAMIFIED, WHERE WILL BRANDS PLAY?

Work can be fun and play can be hard work, but the two are generally seen as separate areas of activity. Finding the right balance between them is currently seen as an essential element of personal well-being.

But for many future consumers, the two domains are likely to merge into one: productive creativity.

Today, young people living in countries with a gaming culture spend an average 10,000 hours playing online games by age 21.That's as much time as they will have spent in compulsory education.

Augmented and virtual realities will become an interactive part of everyday life, across content, media, games and entertainment.

As the technologies involved become more complex and relevant, user experiences will evolve to gamify routine behaviors, transforming the mundane into the spectacular. Media will merge into e-commerce as our "brand experiences" become a growing source of entertainment.

Much of the content that we encounter in this new "digital layer" will be created by future consumers themselves. Everyone will become a producer: remixing content and editing their experiences for the entertainment of others.

Key question: What happens when life is gamified?

Already, we can see micro-influencers and Instagrammers transforming their hobbies and interests into valuable streams of income. They are just the first wave.

Each future consumer will need to find a vocation and a space where they are ready to be "virtually present" day and night.

7. HOW WILL YOU BUILD YOUR CORPORATE CULTURE WHEN YOU DON'T EMPLOY YOUR TALENT?

The notion of a "job for life" is over, and work is increasingly fragmenting. But the nature of work itself is also changing fundamentally.

Sixty-five percent of children starting school this year will assume careers in jobs that don't yet exist. And 57% of jobs in OECD countries are at risk of being replaced by automation.

Future consumers will develop a completely new form of career led by a range of eclectic work experiences, which will combine to help them meet their personal, developmental and financial needs.

Instead of being a potential employee in a fixed-skills workforce, more people will become contractors or freelancers through "cognitive network" platforms.

These platforms will use AI and user data to match projects with people based on expertise, time and wage expectations. They will facilitate personal development, while managing the administrative processes of payment, tax and HR.

Key question: What happens when you don't employ your talent?

Technologies such as virtual reality and AI bots will enable people to perform efficient remote work. But future consumers will often choose shared work environments to maintain social and professional relationships.

Employers will be able to take on a greater variety of tasks, while at the same time reducing their administrative costs.

Governments will collaborate with "cognitive network" platforms to ensure worker rights, keep tabs on the economy and implement automated taxation systems.

8. HOW WILL SMARTER INFRASTRUCTURE SIMPLIFY TRANSPORT?

City planners have been talking about integrated transport infrastructure for decades. Yet for most citizens, getting from A to B can be messy, involving several stages and prone to setbacks like congestion and public transport delays.

Future consumers will use travel services that are better connected and more environmentally friendly. Transport infrastructure will adapt to reflect the travel patterns of its users.

Citizens will have control of their data and will be able to use it to move easily between any transport mode available, within the city or the region. The same would apply to companies moving goods.

This type of data exchange will enable cities to manage traffic flows on an instant, live basis. Transport authorities will capture travel patterns and overall city "busyness," in real time, adapting the tools at their disposal to manage those needs efficiently.

Key question: What happens when travel becomes seamless?

If one in four cars on the road are autonomous by 2030, the number of vehicles that can use a road at one time will increase, as will the scope to reflow traffic. Equally, if more employees are working flexible hours and locations, then peak-time pressure points will lessen.

With greater awareness of how each person's journey is dependent on the travel plans of others, people could fundamentally shift their attitude toward transport. Citizens could focus not on their personal needs, but on "the needs of the system." Today, just 15% of millennials feel it's "extremely important" to own a car.

CONCLUSION

Our eight hypotheses describe deep changes that will fundamentally reshape the lives of future consumers. Exponential changes, by their nature, follow a timeline that is impossible to predict. But the direction of travel is clear. New ways of creating and capturing value will emerge, and companies that get ahead of the curve now will have a clear advantage. How is your organization going to change? ◗

IMPACT ON PHYSICAL WELLBEING

Digital Innovation Today Will Transform Health Care Tomorrow

Need to rebalance the supply-demand scales in health care

Health care infrastructure

India below minimum WHO recommendations for health care workforce and infrastructure

- ~0.6 physicians per 1,000 population
  - 30% below WHO recommendation
- ~1.3 nurses per 1,000 population
  - 50% below WHO recommendation
- ~1.3 beds per 1,000 population
  - 70% below WHO recommendation

~8 in 10 people have no insurance

~7 in 10 people live in rural areas with access to ~30% of health care infrastructure

Health care needs

Noncommunicable diseases constitute

7 out of top **10** **causes of deaths in India**

India accounts for

- >25% of global burden of tuberculosis
- ~20% of global maternal mortality
- ~25% of global infant mortality

Aged population (above 60 years.)

currently ~8% of population

expected to be

~19% of population by 2050

[6] Sources: Medical council of India (MCI), "Healthcare", IBEF, January 2017; "The health workforce in India", WHO, 2016; "Global Tuberculosis Report, 2017", WHO; "Tuberculosis in India," USAID, November 2017; "Non-communicable diseases cause 61% of deaths in India: WHO report", TOI, September 2017; GBD 2016; "5 women in India die every hour during childbirth: WHO", Indian Express, June 2016; "India Among The Top Five Countries Responsible For 50% Newborn Deaths Globally, Despite A 66% Drop In Child Mortality", Indiatimes, October 2017; "India Needs to Start Addressing Issues Concerning Its Growing Elderly Population, Says UN", The WIRE, June 2017

DIGITAL IS ALSO contributing to improved physical wellbeing. Emergence of digital health care and smart devices are assisting in disease prevention and management. With health trackers, people are proactively opting to manage their health and lifestyle. It will not be long before digital therapeutic technology becomes immersive and revolutionizes personal health management.

New health care realities demand new responses

India's health care system is facing the dual burden of rising prevalence of lifestyle-related diseases and aging population. These, combined with the huge population and continued high prevalence of communicable diseases, have put great pressure on

health care infrastructure in India. Hence, it is becoming imperative to use the existing resources in the most efficient and cost-effective manner, while still providing high quality. Digital technologies incorporating the elements of quality, affordability and accessibility, have come to the rescue.

Digital will continue to revolutionize health care delivery systems in the following ways:

Health care will be anywhere, anytime

We are on a journey from health repair to physical wellbeing. As an increasing number of people from smaller cities and villages are getting access to internet connectivity, digital health solutions are connecting them with physicians and reducing the supply-demand gap.

The patients are now able to connect with the physician's 24/7 for acute and chronic diseases without the barriers of distance and cost.

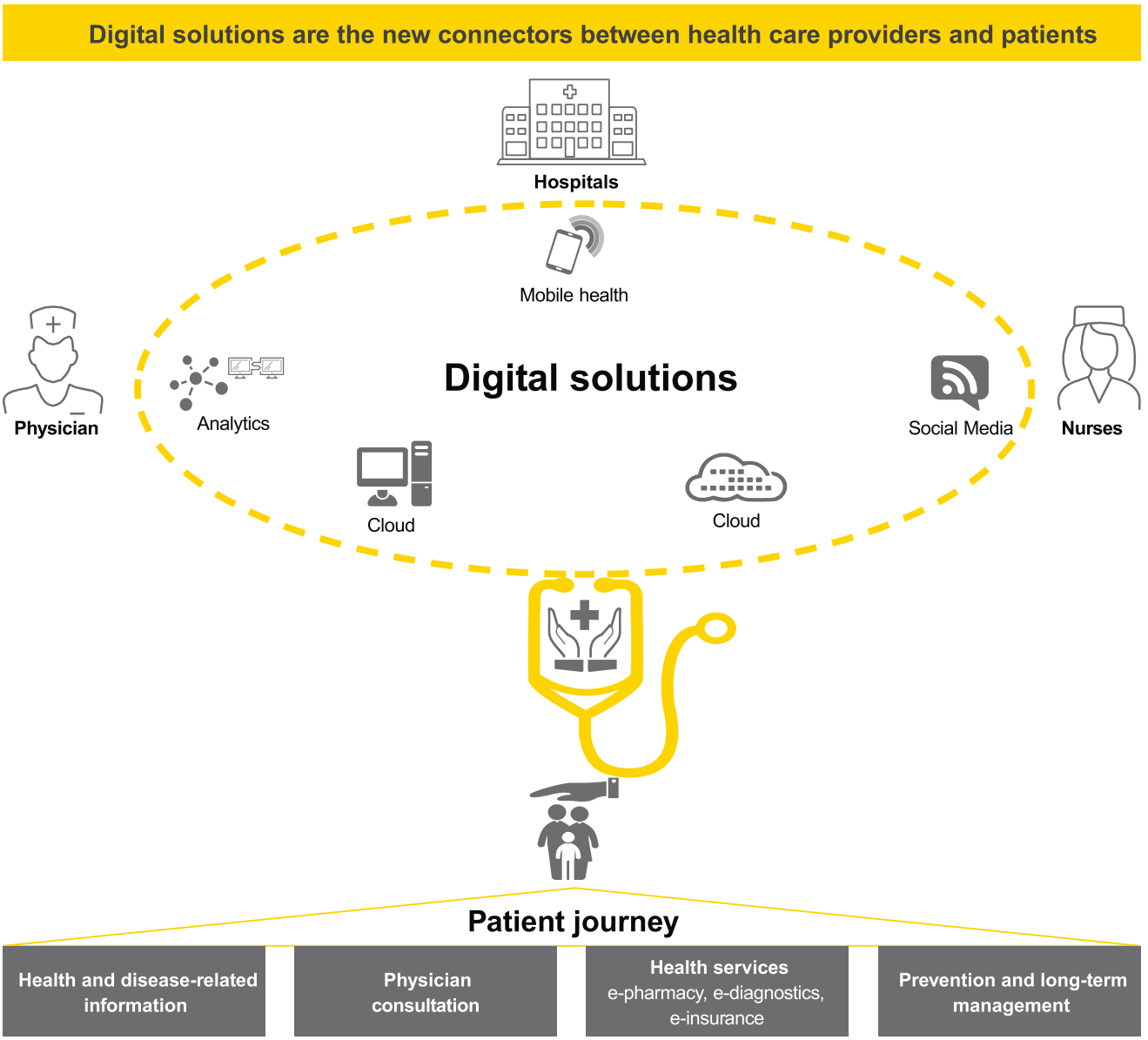
Indian government has already taken the first steps on its revolutionary digital health care journey

The Government's push toward digital is playing a critical role in boosting the digital health care ecosystem in India.

Government playing an active role

Initiatives and incentives	
Startup India: a flagship initiative of the Government of India launched in 2016 that has so far recognized 6,300+ startups	**Reduce medication and medical errors through Integrated Health Information Program (IHIP) and health information exchange**
Policy and regulations	
National Health Policy approved in March 2017. The policy has extensive recommendations on usage of digital health tools and preventive health care	New standards and guidelines for implementation of interoperable **electronic health records** issued in 2016
Setting up of regulatory bodies	
National eHealth Authority (NeHA) to ensure development and promotion of eHealth ecosystem in India	
Launching national level health IT programs (eHealth initiatives)	
Apps and online portals for patient education, disease monitoring and management, integrated disease surveillance, etc.	**SMART Health India program: m-health technologies to** provide health care workers with personalized clinical decision support to guide the Systematic Medical Appraisal Referral and Treatment (SMART)
Information and communication technology (ICT) infrastructure	
Computerization of district and sub-district hospitals, and community health centers to implement the hospital management information system for creation of electronic health record and online prescription	BharatNet (earlier known as National Optical Fibre Network or NOFN): to provide broadband connectivity to all the 2,50,000 Gram panchayats of India. Of this around 1,00,000 Gram panchayats had already been connected by mid of 2017

Digital health is the new response: reshaping health care delivery

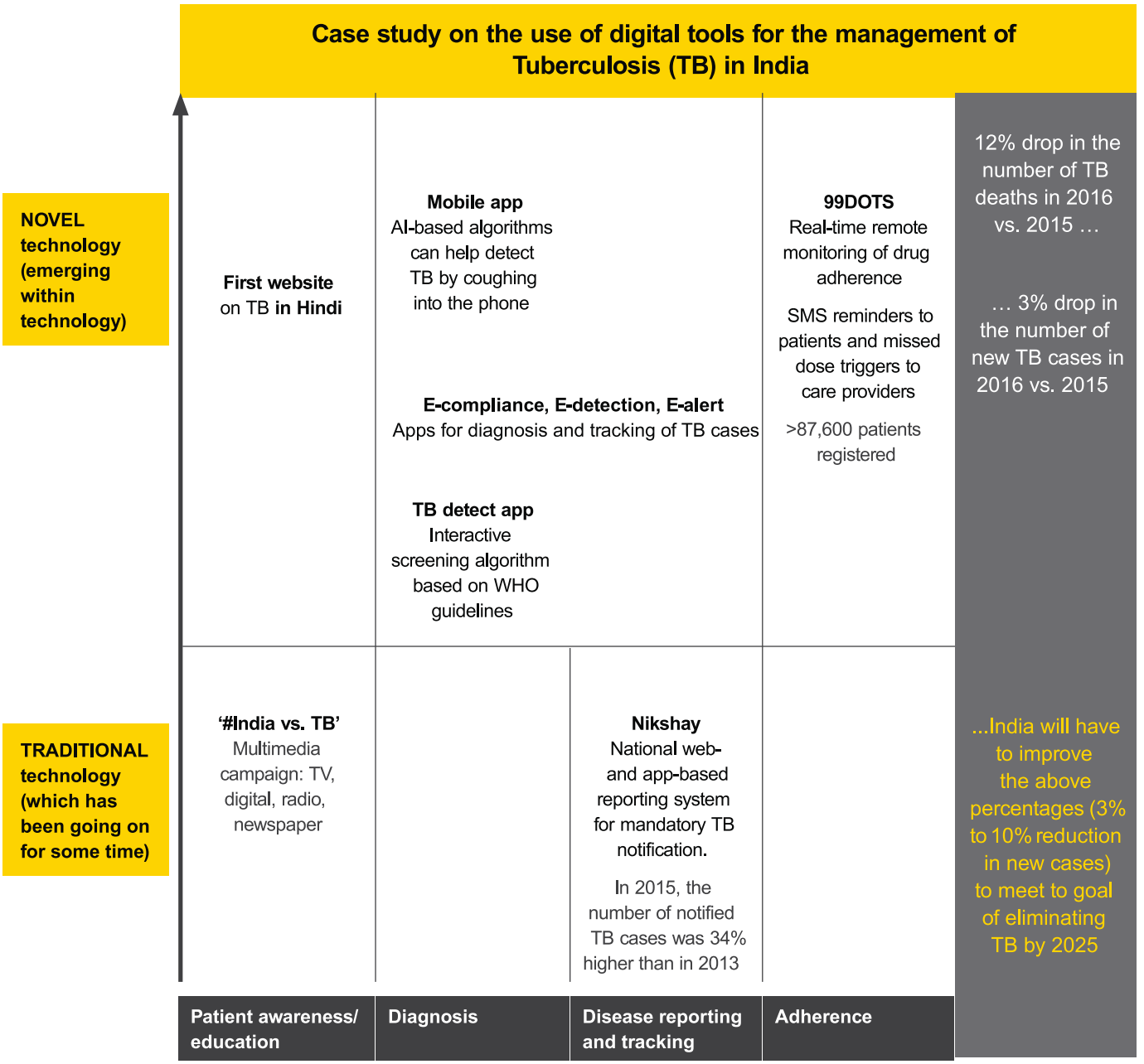


In the future, virtual clinics will offer long-term monitoring of patients in their homes via patient-reported outcome tools. Homes will have replaced hospitals and physicians' offices as the main health care delivery hub. Here is a glimpse of how digital is revolutionizing tuberculosis (TB) care in India.

Mass personalization in care delivery

Health solutions are now becoming available throughout the continuum of patient journey — from collecting information, to interacting with physicians, to ordering medicines and lab tests, to treating and managing disease. With new devices and apps specifically tailored to health care needs in India, it is now possible to monitor patient health at all times, send reminders for medication, receive alerts in case of emergency and encourage healthy habits through digital coaches (such as nutrition and exercise).

The apps and electronic medical records (EMRs) are providing physicians with detailed information about their patients. Data analytics and predictive AI-based algorithms will enable real-time changes in patients' health status to be identified and addressed. Patient care will be personalized — the drugs, solutions and services they receive, their experiences, their interactions with health care professionals and stakeholders, and even where they receive their care. Physicians are also benefitting from the availability of new apps and social platforms where they can share experiences and learn from each other globally.



[7] Sources: WHO; "Tuberculosis in India," USAID, November 2017; "Why Does India Lead The World In Deaths From TB?", NPR, November 2017; "Tracking TB becomes simpler with mobile phone", Down To Earth, May 2017; 99DOTS

Patients will be active partners in managing their own health care

With access to digital health solutions, patients are now evolving from being passive recipients of care to active participants in their own health care. Digital tools (such as mobile apps, wearables and social communities) are equipping them with their own health data, encouraging them to develop the right behaviors and equipping them with the required tools to own their care (e.g., reminders for follow- up with physicians, fill and manage medication, etc.).

To sum up, integrated health care delivery models will become the new reality, provided India continues to march ahead on this transformational journey with an increasing rigor. In this connected ecosystem, 4Ps will become the new normal: painless, prompt, personal and purposeful.

PRIVACY CONCERNS IN THE DIGITAL WORLD

Privacy: Intrinsic right or social construct?

Privacy is entering a time of flux and social norms and legal systems are trying to catch up with the changes that digital technology has brought about. Privacy is a complex construct, influenced by many factors, and it can be difficult to future-proof business plans so they keep up with evolving technological developments and consumer expectations about the topic.

One way to ensure there are no surprises around privacy is by seeing it not as a right, but rather as an exchange between people and organisations, bound by the same principles of trust that facilitate effective social and business relationships.

This is an alternative to the approach of "privacy as right" that instead positions privacy as a social construct to be explicitly negotiated so it is appropriate to the social context in which the exchange takes place.

Isaca notes that enterprises eager to reap the benefits of big data and its vast potential must also recognise their responsibility to protect the privacy of the personal data gathered and analysed with big data. Risk management and maintaining adequate mechanisms to govern and protect privacy need to be major areas of focus in any big data initiative.

The lengthy privacy policies, thick with legalese that most services use now, will never go away, but better controls will, and should, emerge. Whatever tools are used to protect and collect personal data in the future, it will be important for companies such as Facebook and Google to educate their consumers and to provide them with options for all levels of privacy.

7 types of privacy

Privacy of the person encompasses the right to keep body functions and body characteristics (such as genetic codes and biometrics) private;

Privacy of behaviour and action includes sensitive issues such as sexual preferences and habits, political activities and religious practices;

Privacy of communication aims to avoid the interception of communications, including mail interception, the use of bugs, directional microphones, telephone or wireless communication interception or recording and access to email messages;

Privacy of data and image includes concerns about making sure that individuals' data is not automatically available to other individuals and organisations and that people can “exercise a substantial degree of control over that data and its use”;

Privacy of thoughts and feelings refers to the right not to share their thoughts or feelings or to have those thoughts or feelings revealed. Individuals should have the right to think whatever they like;

Privacy of location and space means individuals have the right to move about in public or semi-public space without being identified, tracked or monitored;

Privacy of association (including group privacy) is concerned with people's right to associate with whomever they wish, without being monitored.

Considering the full spectrum of privacy, people must ask themselves: Are you sure you are comfortable with all of yourcharacteristics in the public domain?

For example, do you want people to know where you spend your time - and who you like to spend it with? If you called a substance abuse counsellor, a suicide hotline or a divorce lawyer? What websites you read daily? The religious and political groups to which you belong?

Do We Really Trust Smart Devices?

Some brands are more trusted than others when it comes to smart home devices -- but do these devices really listen to what we say?

– By Eileen Brown

THE GLOBAL SMART home market is forecasted to reach a value of almost $138 billion by 2023, as demand for smart home appliances grows at a high rate. But consumers continue to be suspicious of smart home devices, according to a new report.

In fact, some brands are perceived to be more trustworthy than others when it comes to smart home devices.

Smart devices are here to stay, for sure. They help us stay organized, like with creating grocery lists, making hands-free phone calls, and completing simple tasks.

But we do not trust them completely.

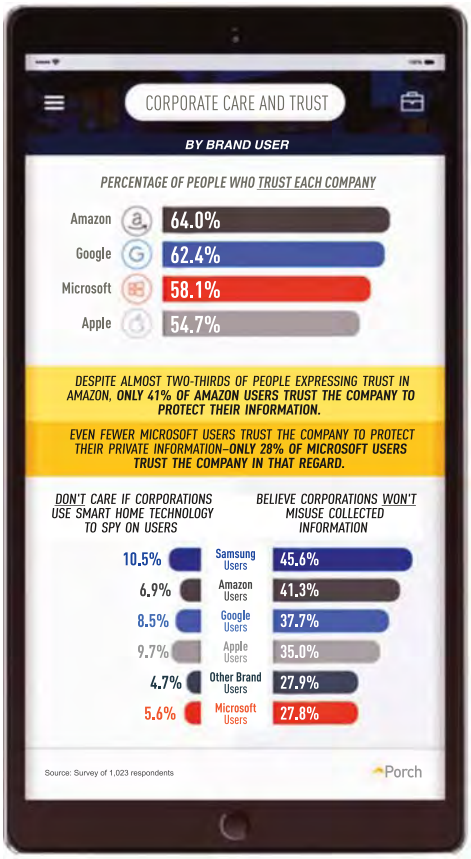
Groups such as millennials feel that they need to have a relationship with a brand before buying the latest technology.

Although they are influenced by the buzz around a new device and want to be involved, they do not fully trust their devices.

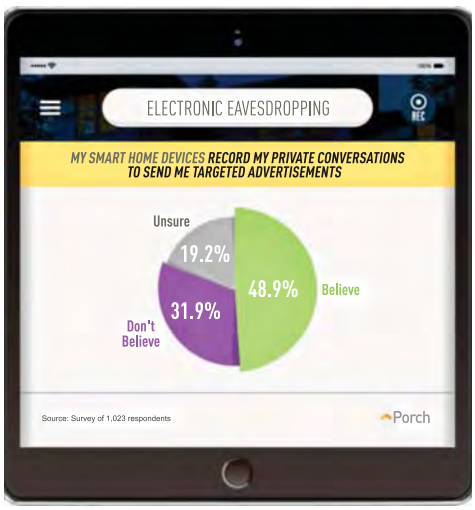
Over half of respondents own smart devices (57.4 percent of baby boomers, 69.6 percent of generation X, and 75.1 percent of millennials). But less people actually trust their devices.

Thirty-four percent of smart home device owners do not trust their devices -- nor device manufacturers.

Amazon leads the way with consumer trust, with almost two-thirds (64 percent) of respondents trusting the company.Apple held the lowest score, with 54.7 percent trusting the company. Nearly half of respondents believe their smart home devices are recording their private conversations for targeted ad use, even though Google and Amazon deny any such claim.



(Image: Porch)



Over one in five (22 percent) of respondents who own smart speakers reckon that their device has refused to follow their commands, and sadly, seven percent of Amazon Alexa users are convinced their device has randomly laughed at them.

Although smart home technology is in its early stages, and we do not implicitly trust it, adoption is on the rise.

We still have much to learn about how it will impact our society for generations to come, and as it becomes more sophisticated, we will need to become smarter, too.

With the recent focus on AI technology and bots, do we prefer interacting with the most human-like assistants?

Social media platforms must evolve to higher privacy standards -- to stop their users leaving for more secure channels.

10 Breakthrough Technologies That Are About To Change The World

The future is coming faster than you think. You need to prepare.

CREDIT: Getty Images

ANY FOOL ON the street can tell you that technology is changing at a whiplash-inducing pace. What's much more difficult to predict is which technologies specifically are about to hit big. Manage to divine that information before the rest of the crowd and you can future-proof your career and get in early on some of the coolest (and most lucrative) business opportunities.

Of course, sorting through a pile of tech hype to find these nuggets of tech gold is one of the hardest jobs around. It demands not only a ton of specialized knowledge but also an uncanny ability to sense which way the cultural winds are blowing.

Thankfully, some of the smartest minds in the world are willing to help out, offering periodic lists of technologies that are about to change the world. One of the best is from MIT Technology Review, which has been naming breakthrough technologies to watch for 15 years now. Here are the picks:

1. Reversing Paralysis

."Scientists are making remarkable progress at using brain implants to restore the freedom of movement that spinal cord injuries take away."

2. Self-Driving Trucks

."Tractor-trailers without a human at the wheel will soon barrel onto highways near you. What will this mean for the nation's 1.7 million truck drivers?"

3. Paying With Your Face

. "Face-detecting systems in China now authorize payments, provide access to facilities, and track down criminals. Will other countries follow?"

4. Practical Quantum Computers

."Advances at Google, Intel, and several research groups indicate that computers with previously unimaginable power are finally within reach."

5. The 360-Degree Selfie

. "Inexpensive cameras that make spherical images are opening a new era in photography and changing the way people share stories."

6. Hot Solar Cells

."By converting heat to focused beams of light, a new solar device could create cheap and continuous power."

7. Gene Therapy 2.0

. "Scientists have solved fundamental problems that were holding back cures for rare hereditary disorders. Next we'll see if the same approach can take on cancer, heart disease, and other common illnesses."

8. The Cell Atlas

."Biology's next mega-project will find out what we're really made of."

9. Botnets of Things

. "The relentless push to add connectivity to home gadgets is creating dangerous side effects that figure to get even worse."

10. Reinforcement Learning

"By experimenting, computers are figuring out how to do things that no programmer could teach them."

SOURCES / REFERENCES

consuersinternational.org
exlservice.com
researchgate.net
weforum.org
information-age.com
digitalistmag.com
capgemini.com
deloitte.com
Forbes.com
inc.com
cms-connected.com
sciencedirect.com
pewinternet.org
computerweekly.com
comscore.com
link.springer.com
digitalmarketinginstitute.com
indiabriefing.in
rccp.gov.in
digitalterminal.in
techradar.com
livemint.com
Manu Balachandran
Indian express
Times of India
Economic Times
idc.com
statista.com
ifihomes.com
Deccan chronical
gs1india.org
meity.gov.in
lifehacker.com
copperhorse.co.uk
tcs.com
TechCrunch.com
pfile.com
smartcities.gov.in
iotforall.com
ibm.com
Iotagenda.techtarget.com
techopedia.com
theguardian.com
india.gov.in

Amway™

DIGITAL BHARAT.
DIGITAL AMWAY.
#AbRuknaNahinHai

50,00,000
NEFT transactions
processed to Amway Direct Sellers in a year

Partnership with ITZ prepaid cards
Forged a partnership with ITZ prepaid cards six years ago to digitise cash transactions

ATM enabled purchases
Bank ATMs enrolled for Amway product purchases

95% collections went digital
in November, including 3,00,000 active orders processed via debit, credit, ITZ pre-paid cards & Net Banking

NACH enabled product purchases
in the North-East

Mandatory KYC
Bank account and Aadhaar KYC made mandatory for appointment as an Amway Direct Seller

100% digital payments
100% of vendor and employee payments happen digitally

Amway India's state-of-the-art manufacturing facility in Nilakottai, Tamil Nadu.

CUSTOMER SATISFACTION 100% OR MONEY REFUNDED

Join us on facebook@ /amwayindiaofficial or follow us on twitter@ /amwayindia
For more details; please visit us at www.amway.in

Posted at Lodi Road HPO, New Delhi on 9-10th of every month
Published on 6th of every month

RNI No. DELENG/2015/67140
REG. NO. DL (S)–17/3523/2017-19

4,55,000+ HAPPY CONSUMERS

Together WE CAN make a difference

JAGO GRAHAK JAGO

Jagograhakjago.com

Toll free # 1800-11-4424

Consumer Conexion

CONSUMER ONLINE FOUNDATION

www.ConsumerOnlineFoundation.org

35 YEARS 1983-2018 IN THE CONSUMER MOVEMENT

www.bejonmisra.com

Printed, published & owned by Bejon Kumar Misra, Printed at M/s. Swastika Creation, 19, D.S.I.D.C. Shed, Scheme 3, Okhla Phase II, New Delhi - 110020 and Published at B - 306, 1st Floor, C.R. Park, New Delhi-110019,
Editor: Pooja Khaitan