Assessing Regulatory Requirements of Privacy Management for Members Offering IoT Services Using Personal Data

November 2018

Table of Contents

1. Executive Summary

- Recent policymakers and regulators revisions of privacy rules and frameworks respond to growing concerns about how to best protect citizens' privacy when new services and technologies pose ever more complex and sophisticated challenges.

- The GSMA's work in mobile privacy is still very relevant to guide all services, including IoT and big data services, towards conformity with new rules. The fundamental underlying privacy principles that need be addressed in the face of new frameworks remain unchanged: openness and transparency towards users, data minimisation, limited purpose and use of data - providing users choice and control. These principles are reflected in the *GSMA Mobile Privacy Principles*[1], which describe how mobile consumers' privacy should be respected and protected when they use mobile services and applications.

- IoT services present specific challenges: there will be millions of connected devices deployed in the field, and they will be very diverse in their functionality and data handling. Some devices may be considered as non-personal while still capturing personal data, and some may pose specific security risks and compromise privacy indirectly. Also, new rules that impose very short time periods for reporting breaches may present challenges for IoT devices in the field with no regular human control. Finally, operators deploying IoT solutions in partnership with other parties must consider the risk of reputational damage that may arise when those parties are in breach, but the service can still be associated with the operator's brand. Reputational damage may be a lot more significant than new hefty fines that new rules impose.

- In the EU, the *General Data Protection Regulation* (GDPR) came in to force on 25th May 2018 and is increasingly seen as a new global standard for privacy. One important overarching element of the GDPR is its focus on accountability and a "risk-based approach". It enhances obligations with the goal of ensuring that organisations actively take demonstrable steps to mitigate privacy risks.

- Still in the EU, the Alliance of IoT Industries (AIOTI), identified thirty baseline principles regarding security and privacy. Many of these apply across different IoT domains and focus on transparency, user control and integrating privacy-by-design. These are reported in *Annex*.

- In the USA, privacy is enforced by the FTC under the FTC Act's prohibition of unfair and deceptive acts or practices. Some states have also enacted privacy legislation - such as the California Consumer Privacy Act of June 2018, which sets out a very broad definition of personal data and new hefty fines.

- In Japan, the recently revised *Act on the Protection of Personal Information* (APPI) reinforced already existing measures. Notably, in July 2018 Japan and the EU formally recognised each other's data protection systems. This is a first step towards full adequacy and it is expected to be finalised by the end 2018. This will pave the way for creating the world's largest zone in which personal data is allowed to flow freely and consumers' privacy is protected at a high standard.

[1] GSMA (2016). *Mobile Privacy Principles*. Available at: https://www.gsma.com/publicpolicy/wp-content/uploads/2016/02/GSMA2016_Guidelines_Mobile_Privacy_Principles.pdf

- Brazil and India have recently considered new data protection rules. The proposed Indian law introduces new obligations on the so-called '*Data Principal*' as the subject processing data for any individual. It also defines a class of "*Critical Personal Data*" considered so strategic that cannot be transferred out of the country and will have to be processed only in India.

- Members wanting to launch IoT and big data services should focus on three areas requiring special attention. We identify these areas with three questions: (i) When IoT data is considered personal? (ii) Who is the data controller? (iii) How end users can express choice and consent on their data? For each area we provide explanatory examples and additional sub-questions to help the process. A subsequent GSMA report "Protecting Privacy in the IoT" will focus on the techniques that can be used to practically address these challenges.

2. Introduction

This paper aims at documenting and assessing regulatory requirements for members offering IoT services utilising personal data. We look into the privacy regulatory requirements in some key jurisdictions likely to influence other regulatory regimes around the world: the EU, the USA, Japan, India and Brazil. We then identify what, in light of the existing rules, the likely upcoming privacy regulatory challenges will be.

This paper should be read in conjunction with the GSMA technical document "Protecting Privacy in the IoT", expected to be published by December 2018, which elaborates on techniques such as anonymisation, pseudonymisation, aggregation, encryption, k-anonymity and differential privacy that are being used to address privacy requirements.

In the section "IoT Market Characteristics" we identify the particular aspects of IoT services which constitute challenges for privacy compliance. In the "Global Regulatory Developments" section, we cover the latest privacy regulation developments in the EU, the USA, India, Japan and Brazil. Finally, in the section "Considerations for Applying Privacy Principles for IoT" we focus on the three key questions that are central to IoT and privacy:

(i) When data is considered personal?
(ii) Who is the data controller?
(iii) How to express consent?

Addressing these three questions requires thoughtful consideration, and the right approach will vary from service to service, however the high-level underlying principles remain unchanged.

GSMA privacy principles remain valid guidelines to follow

In recent years, policymakers and regulators have more intensively focused their efforts and activities in guaranteeing people's privacy while using digital technologies and services. The common tendency to rethink and revise existing privacy rules and frameworks responds to growing concerns about how to best protect citizens' privacy in a rapidly changing world, where new services and technologies pose ever more complex and sophisticated challenges. As we observe these developments, we note that the GSMA has already done significant work in the area of mobile privacy principles. We believe that the fundamental underlying principles that need to be addressed to provide appropriate privacy protections remain to a large extent unchanged; some of these principles are and will be still particularly relevant for IoT:

- **Openness, transparency and notice:** Users should be provided with information about organisations collecting personal information about them, why such information is collected, for which application or service, and what happens afterward, i.e. sharing and further use of their data. This will help them make informed decisions about whether or not to use an IoT service.
- **Data minimisation and retention**: Only the minimum personal information necessary to meet legitimate business purposes and to deliver, provision, maintain or develop applications and services should be collected. Personal information must not be kept for

longer than is necessary for those legitimate business purposes or to meet legal obligations and should subsequently be deleted or rendered anonymous.

- **Purpose and use**: The access, collection, sharing, disclosure and further use of users' personal information shall be limited to meeting legitimate business purposes, such as providing applications or services as requested by users, or to otherwise meet legal obligations.
- **Users' choice and control:** Users shall be given opportunities to exercise meaningful choice and control over their personal information.

3. IoT Market Characteristics Posing Specific Privacy Challenges

a. **Number of devices**: IoT is and will predominantly be a business of scale. Members addressing the IoT opportunity will want to serve thousands or millions of devices, possibly across many countries. GSMA Intelligence estimates that there will be over 25 billion IoT connections by 2025 globally, out of these three billion will be connected by licensed cellular IoT and the rest via other types of connectivity e.g., Wi-Fi, fixed lines.

   In practice, IoT architectures will often combine short range and wide area connectivity. For example one single wide area cellular connection serving a gateway. The gateway then connects many '*Smart Home*' devices via short range connectivity such as Bluetooth. Regardless of the chosen architecture, some devices will be capable of capturing, storing, processing and actuating upon data received or sensed.

   Other devices will sense specific attributes of an environment, such as a smart kettle sensing a temperature to allocate energy, and this reading could be combined with data from other sensors to monitor overall energy usage. Any device will potentially present a privacy challenge if it processes or stores personal data. Managing the sheer number of active devices at one time, being in control of all of them, their location, the information that they store represents a primary privacy challenge.

b. **Diversity of devices**: Identifying and mitigating privacy risks can be especially challenging given the ever expanding number of manufacturers and types of devices and the diverse range of IoT device capabilities. Design and functionality can also impact privacy considerations, for example because many IoT devices may not have a direct user interface. This may require new ways of thinking about the privacy principles of notice, choice and transparency.

c. **Non-personal devices tracking personal data:** Unlike traditional voice and data services, IoT devices may be, depending on the specific application, loosely related with one single individual. For example, a smart parking device embedded in the street pavement; a smart sensor measuring the amount of litter contained in a roadside bin; or in the context of smart agriculture, a passive infra-red movement sensor to detect the presence of workers in a grain silo.

   All of these devices may not be considered as strictly personal as they either do not belong to a single user and do not track information specifically related to an identifiable individual: i.e., whether a parking space is busy, whether a bin is full, or whether a worker is operating in safe conditions or not.

   However, this information, if combined and associated[2] with a device's contextual information, such as location or metadata, or publicly available information and can be used to identify a specific person or gather meaningful personal information.

[2] With such combination and association happening at a 'higher' application level.

To follow on the above examples, the smart parking sensor may reveal the driver and car location, a 'personal' smart bin can disclose whether the residents of a house have been at home or on vacation, and an IoT sensor tracking movement on-site may provide information about the workers' time at work or their efficiency.

Inferred data *may* therefore be personal and *may* fall under privacy rules. A third, specific privacy challenge consists therefore in assessing IoT captured data not only independently but within their context and metadata.

d. **Reporting breaches in time**: New privacy rules require reporting privacy breaches in a very short time frame. For example, in Europe, the General Data Protection Regulation (GDPR) sets out a 72 hours window. Breaches are difficult to identify because often they will be created by hackers who conceal their tracks. For IoT devices it can be even harder as they are deployed in the field and track data through fully automated mechanisms. While some of this data might be acted upon immediately, it is likely that other data will be stored as part of a historical record or analytics and actuation may happen at a deferred point in time.

   Some of this data may indeed be personal. Therefore a fourth challenge is to have visibility on what data is being generated and stored by sensors, including maintaining an up-to-date logs and mapping of devices generating personal data sources, their location and data lifecycle, to identify and report private data breaches in time.

e. **Security risks:** Many IoT devices are designed to have low power consumption, to be low complexity/low cost, to have a long lifecycle duration and to operate outdoors. Low cost IoT devices may have limited cryptographic capability, small memory and constrained operating systems. The result is that the device may be unable to perform 'internet-grade' cryptography or contain 'secure hardware', and they could be subject to physical or localised attack which could compromise the security and privacy of data stored in them.

   Long device lifetime also means that should vulnerabilities be identified, the potential risk stays in place for many years unless the devices are appropriately patched or upgraded. This creates a requirement for flexible bandwidth two-way communications. Mobile IoT technologies such as LTE-M or NB-IoT can effectively fulfil this requirement.

   Finally, outdoor deployment means hackers could more easily physically access the device and compromise its integrity, e.g., through removing a flash memory card. A fifth privacy challenge consists therefore in developing appropriate defence strategies against both physical and online attacks by implementing the so called security-by-design.

f. **Complex value chains and risk of reputational damage:** Mobile operators may be deploying IoT services in collaboration with partners (e.g., device vendors, systems integrators, application developers). Each player must comply with privacy rules while exchanging and processing data through different platforms. For end-to-end privacy to be guaranteed across complex architectures and value chains all elements must be compliant.

   The reputational risk for larger companies should also be taken into account as the impact could be much wider than fines itself and felt throughout the business. A sixth privacy challenge consists in ensuring third parties involved in the provision of IoT services are accountable for protecting privacy, to avoid reputational damage and to sustain consumer trust.

4. Global Regulatory Developments – Focus on IoT Services Using Personal Data

4.1 EU

GDPR

On May 25, 2018, the EU General Data Protection (GDPR) entered into application. The GDPR significantly changed the landscape of privacy regulation in the European Union (EU) and across the world. The GDPR applies to the processing of personal data of people in the EU, and also applies to organisations outside of the EU offering goods and services to people in the EU[3], or monitoring the behaviour of people in the EU.[4] This jurisdictional reach means that any organisation intending to market goods and services, including IoT devices and services, to people within the EU, must comply with the GDPR.

The GDPR expands on elements of its predecessor legislation - the 1995 EU Data Protection Directive, and introduces some new concepts. For example, the GDPR clarified that consent for the collection and processing of data must be freely given, specific, informed, and unambiguous.[5]

The GDPR also expands subject access rights to include the right to erasure (i.e., "the right to be forgotten") and the right to data portability. Amongst other changes, the GDPR also establishes new mechanisms for transferring data outside of the EU, created a "one-stop shop" mechanism to clarify enforcement responsibility, and established new penalties of up to four per cent of global annual turnover.

One important overarching element of the GDPR is its focus on accountability and a "risk-based approach". The GDPR requires that organisation apply a data protection by design and default

[3] The following practices may constitute the "offering goods and services" to people in the EU:
-Use of a language used in one or more EU Member States with the possibility of ordering goods and services in that other language (Recital 24 GDPR)
-Use of a currency used in one or more EU Member States (Recital 24 GDPR)
-The mentioning of customers or users who are in the Union (Recital 24 GDPR)
-Paying a search engine to target users in the EU
-Using an EU country code (e.g. .eu or .de)
-Using an EU telephone number

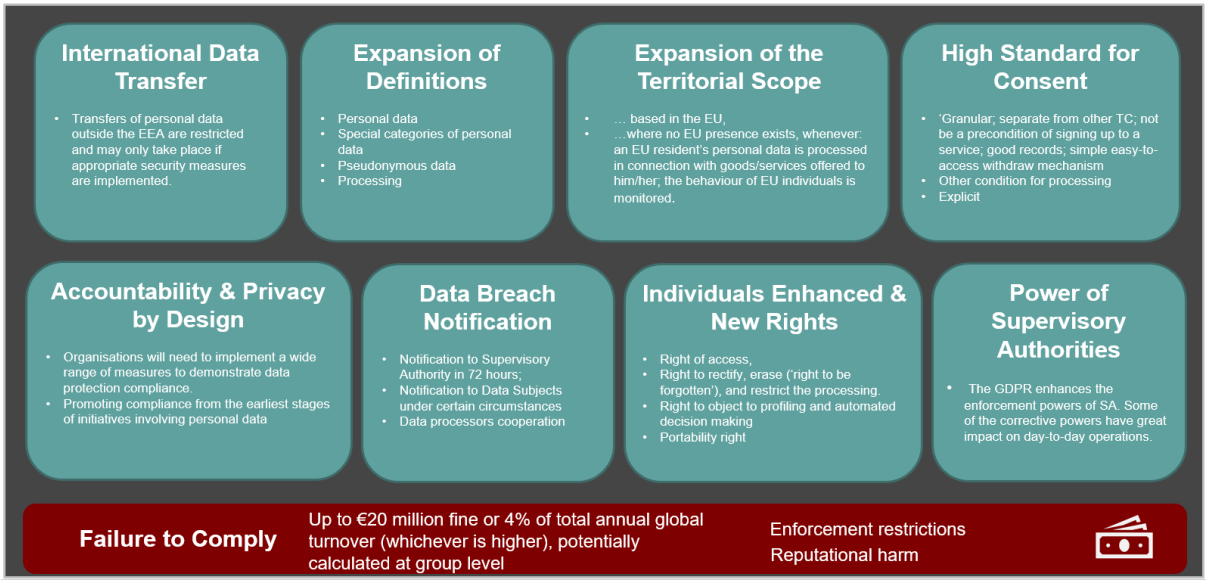
[4] Tracking natural persons on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes. Potentially including, for example: online behavioural advertising, risk assessments including credit scoring, tracking users through mobile apps including mapping apps, use of fitness trackers.

[5] The consent standard in the GDPR is often described as "explicit," but this reflects misunderstanding. In the GDPR, explicit consent is reserved for the processing of "special categories" of data, more widely known as "sensitive categories" of data. Explicit consent, while similar to "informed consent", requires a written statement, or an electronic act such as filling in a form. 5. EC (2018). *Article 29 Working Party Guidelines on consent under Regulation 2016/679.* Available at: http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030

approach, and requires that organisations conduct data protection impact assessments in certain cases.

The GDPR also enhances obligations regarding documentation of privacy practices, with the goal of ensuring that organisations take demonstrable steps to mitigate privacy risks.

GDPR Key Elements:



Source: GSMA

The GDPR is an omnibus legislation - it is sector and technology-neutral. The requirement to implement data protection by design- integrating privacy risk mitigation measures throughout the product/service lifecycle will apply to the Internet of Things (IoT) ecosystem. Data protection by design will help identify considerations and risks specific to the IoT.[6]

ePrivacy Regulation

In the EU, the ePrivacy Directive applies to the confidentiality and privacy of electronic communications data. In January, 2017, the European Commission (EC) released a proposal for an updated ePrivacy Regulation (ePR)[7]. In the EC's proposed text, Recital 12 notes that the proposed ePR should apply to the transmission of *machine-to-machine communications*, with the stated goal of promoting a trusted and secure IoT.

[6] GSMA (2012) *Privacy Design Guidelines for Mobile Application Development*. Available at: https://www.gsma.com/publicpolicy/privacy-design-guidelines-mobile-application-development
[7] EC (2017) *Proposal for a Regulation of the European Parliament and of the Council*. Available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241

Article 8 of the ePR would prohibit the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment except on the following grounds:

> a) It is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or
>
> b) The end-user has given his or her consent; or
>
> c) It is necessary for providing an information society service requested by the end-user (such as making an mobile phone app working); or
>
> d) If it is necessary for web audience measuring, provided this is carried out by the provider of the information society service requested by the end-user.

Article 8 would also prohibit the collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment unless the purpose is to establish a connection, or a clear and prominent notice is displayed, consistent with Article 13 GDPR.[8]

Many uses of IoT data will fall under the exceptions for "information society services" (ISS)[9] Some IoT services may be considered "electronic communications services," (ECS) which means that other parts of the ePR may also apply, including Article 6, which would prohibit the processing of communications metadata except for a few narrow exceptions:

a) Transmission of the communication, to maintain or restore the security of networks and services, or
b) Detect technical faults and/or errors in transmission, billing, calculating interconnection payments,
c) Detecting or stopping fraudulent, or abusive use of ECS, or
d) On the basis of consent, if the purposes of processing could not be fulfilled by processing anonymised information.

To determine whether an IoT service is an ISS or ECS, in its February 2016 Report "*Enabling the Internet of Things services*", the Body of European Regulators for Electronic Communications (BEREC) stated that:

> "*Services in the IoT value chain generally depend on a connectivity service as an input product but connectivity accounts for a relatively low proportion of the overall revenue opportunity in the IoT value chain. Hence, in many cases it is decisive whether the respective service in the IoT value chain consists "wholly or mainly" in the conveyance of signals on electronic communication networks. This criterion leaves room for interpretation. Due to the variety of IoT services, this assessment may often only be possible on a case-by-case basis. This assessment may be made by an NRA, whose decision, however, may be subject to review by national courts and finally the ECJ.*

[8] The European Parliament and the Council of the European Union (2016) *The EU General Data Protection Regulation, article 13.* Available at https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A13
[9] Hogan Lovells (2017) *Draft e-Privacy Regulation End users' terminal equipment rules*. Available at: https://www.hldataprotection.com/files/2017/01/Draft-e-Privacy-Regulation-End-users-terminal-equipment-rules.pdf

It is helpful to assess the respective service (contract) in the value chain in order to determine whether it can be qualified as an ECS.

Within the IoT value chain, the connectivity service provider (e.g. the mobile operator) who provides connectivity over a public network for remuneration is generally a provider of an ECS.[10]"

The EU institutions continue to negotiate the proposed ePR. The European Parliament agreed on a negotiating position on the proposed ePR in October 2017. The European Council's debate on the legislation will continues, but the Austrian Presidency proposed new amendments to the ePR on 10 July 2018.[11]

In its proposed amendments, in a new Article 6(2a), the Austrian presidency included a new basis for processing communications metadata by ECS for "*further compatible processing"* subject to mandatory safeguards, including pseudonymisation.

The Austrian Presidency proposed amendments to Article 8 which would also permit the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment in order to provide security updates and to maintain and restore the security of information society services.

The Austrian Presidency proposed amendments to this requirement stating that consent and statistical counting could also be a basis for the collection of information emitted by terminal equipment to enable it to connect to another device and/or to network equipment. EU Member States did not agree to the proposed amendments, so the Austrian Presidency will reconvene discussions on the ePR on 27 September 2018.[12]

Other sources

The European Commission is interested in examining baseline privacy principles for IoT. The EC, working with AIOTI, convened a workshop on IoT Security and Privacy in January 2017.[13] The results of the workshop showed an aggregated thirty (30) minimum baseline principles regarding either security or privacy across different IoT domains.[14] Many of the privacy principles for the different IoT domains are similar, and focus on transparency, user control (and data control, e.g. assessing who is responsible for which uses of data across the IoT ecosystem), and integrating Privacy by Design.

[10] BEREC (2016) *Report on Enabling the Internet of Things*, page 21. Available at: https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/5755-berec-report-on-enabling-the-internet-of_0.pdf
[11] Council of the European Union (2018) *Document 10975/18*. Available at: https://iapp.org/media/pdf/resource_center/ePR-draft-July-2018.pdf
[12] At the time of writing this is the latest information available
[13] EC (2017) *Report on Workshop on Security & Privacy in IoT, Annex 1.* Available at: http://ec.europa.eu/information_society/newsroom/image/document/2017-15/final_report_20170113_v0_1_clean_778231E0-BC8E-B21F-18089F746A650D4D_44113.pdf
[14] See Annex 1 to this report
[15] EC (2014) *Article 29 Working Party Opinion 8/2014 on the on Recent Developments on the Internet of Things.* Available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

The Article 29 Working Party (which consisted of the data protection authorities from each EU Member State, and has seen been replaced by the European Data Protection Board) also addressed IoT privacy in their 2014 opinion.[15] This document specifies the Working Party's main IoT privacy challenges and includes recommendations for IoT privacy. The main challenges identified are:

1) Lack of control and information asymmetry;

2) Quality of the users' consent;

3) Inferences derived from data and repurposing of original processing;

4) Intrusive bringing out of behaviour patterns and profiling;

5) Limitations on the possibility to remain anonymous when using services;

6) Security risks: security vs. efficiency.

To mitigate these risks, the Working Party made the following recommendations:

- Privacy Impact Assessments (PIAs) should be performed before any new applications are launched in the IoT.
- Many IoT stakeholders only need aggregated data and have no need of the raw data collected by IoT devices. Stakeholders must delete raw data as soon as they have extracted the data required for their data processing. As a principle, deletion should take place at the nearest point of data collection of raw data (e.g. on the same device after processing).
- Privacy by Design and Privacy by Default should be implemented by all stakeholders
- User empowerment- data subjects and users must be able to exercise their rights and thus be "in control" of the data.
- Methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible.
- Devices and applications should also be designed so as to inform users and non-user data subjects, for instance via the device physical interface or by broadcasting a signal on a wireless channel."

While this Opinion pre-dates the GDPR, much of the guidance remains relevant as it is based on widely-accepted privacy principles (e.g., user choice and control, transparency, data minimisation). The guidance also refers to a 2013 Working Party Opinion on Smart Devices, which includes similar guidance, broken down into recommendations for app developers, app stores, OS and device manufacturers, and third parties.[16]

[15] EC (2014) *Article 29 Working Party Opinion 8/2014 on the on Recent Developments on the Internet of Things.* Available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.
[16] EC (2013) *Opinion 02/2013 on apps on smart devices.* Available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

4.2 USA

Federal Trade Commission

The general Federal Trade Commission privacy (and data security) enforcement authority is based on authority to enforce against "unfair or deceptive acts or practices".

In the United States, privacy is regulated on multiple levels- including Federal sectoral law and regulation and laws in individual states. The U.S. Federal Trade Commission (FTC), the administrative agency responsible for protecting consumers and promoting competition, enforces against "unfair or deceptive acts or practices in or affecting commerce", pursuant to Section 5 of the FTC Act.[17] Although the FTC has authority over most companies, there are certain jurisdiction exclusions, such as common carrier activities.[18] For example, the U.S. Federal Communications Commission regulates some aspects of consumer privacy in the context of telecommunications common carrier activities[19].

In many cases, the FTC's enforcement of privacy under the FTC Act's prohibition of "deceptive acts or practices" focuses on the premise that companies making public promises to protect privacy must uphold these promises.[20] In other cases, the FTC's enforcement is based on "unfair" acts or practices.

For example, as noted in an FTC press release, the smart TV manufacturer VIZIO, agreed to pay $2.2 million to settle charges by the Federal Trade Commission and the Office of the New Jersey Attorney General that it installed software on its TVs to collect viewing data on 11 million consumer TVs without consumers' knowledge or consent.[21]

The Complaint stated that VIZIO "*failed to adequately disclose that the 'Smart Interactivity' feature comprehensively collected and shared consumers' television viewing activity from cable boxes, DVRs, streaming devices, and airwaves, which Defendants then provided on a household-by household basis to third parties*", and that this behaviour was deceptive, allegedly violating the FTC Act. The FTC also alleged that VIZIO had "*represented expressly or by implication that [VIZIO] would provide program offers and suggestions to consumers with 'Smart Interactivity' enabled on their televisions*." According to the Complaint, however, VIZIO did not provide program offers or suggestions to those consumers, which the FTC alleged was a deceptive practice. The FTC also alleged that certain of Vizio's practices were "unfair."

Other "sectoral" privacy legislation enforced by the FTC includes the Children's Online Privacy Protection Act (COPPA), and the Gramm Leach Bliley Act (GLBA) (covering certain financial institutions). Other prominent sectoral privacy regulation in the U.S. includes the Health Insurance

[17] 15 U.S.C. § 45. (For an unfair act or practice to violate Section 5 of the FTC Act it must "cause or [be] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." Additionally, deception requires a material representation, omission, or practice that is likely to mislead consumers, who are acting reasonably under the circumstances. See Fed. Trade Comm'n, Policy Statement on Deception (Oct. 14, 1983).
[18] T John Eggerton (2018) Ninth Circuit Clarifies: FTC Common Carrier Carve-Out Is Activity Based. Available at: https://www.broadcastingcable.com/news/ninth-circuit-clarifies-ftc-common-carrier-carve-out-activity-based-172046
[19] Legal Information Institute (2017) *Customer Proprietary Network Information regulation*: https://www.law.cornell.edu/cfr/text/47/part-64/subpart-U
[20] Federal Trade Commission (2018) *Privacy and Security Enforcement, Press Releases.* Available at: https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises
[21] Federal Trade Commission (2017) *VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent.* Available at: https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it

Portability and Accountability Act (HIPAA), enforced by the U.S. Department of Health and Human Services, and the U.S. Privacy Act, which covers privacy rules for Federal government use of data.

In 2013, the FTC hosted a workshop entitled *Internet of Things: Privacy & Security in a Connected World*.[22] The workshop brought experts together to talk about the potential privacy risks associated with IoT and how organisations can mitigate those risks. In 2015, the FTC issued a report summarising the workshop discussions, and providing FTC staff's recommendations on protecting privacy in the IoT. [23]

To spur innovative mechanisms for reducing risk, in January 2017, the FTC announced an "Internet of Things Challenge" to combat security vulnerabilities in Home Devices- the winner, Steve Castle, developed a mobile app called "IoT watchdog", a tool to help consumers scan their home networks to identify and update devices.

Also in January 2017, the FTC filed a complaint against D-Link, and the FTC noted in the press release that the company "put[ting] consumer privacy at risk due to inadequate security of its computer routers and cameras."[24] The FTC also settled an action with ASUS and the FTC noted in its press release that "critical security flaws in its routers put the home networks of hundreds of thousands of consumers at risk."[25] The FTC also settled an action with TRENDnet and the FTC noted in its press release that this "marketer of Internet-connected home security video cameras…failed to protect consumers' privacy."[26]

In recent testimony to the U.S. Consumer Product Safety Commission, the FTC recognised the proliferation of connected devices, and the myriad benefits these devices offer to consumers, while also noting that the benefits of connective devices "*may be foreclosed if IoT devices themselves are a hazard*."[27] In this testimony, the FTC maintained that "*companies that manufacture and sell IoT devices must take reasonable steps to secure them from unauthorized access*." These reasonable steps include exercising oversight of a third party providing services[28].

State-level legislation

Some U.S. States have passed privacy legislation- primarily applying to specific sectors or groups of individuals (such as children, which are subject to special laws in California and Delaware).[29]

---

[22] Federal Trade Commission event page (2013*): Internet of Things - Privacy and Security in a Connected World* workshop, available at: https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world

[23] Federal Trade Commission (2015) *Internet of Things Privacy & Security in Connected World.* Available at: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[24]Federal Trade Commission (2017) Press Release: *FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras*, available at: https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate

[25] Federal Trade Commission (2016) Press Release: *ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk*, available at: https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put

[26] Federal Trade Commission (2013) Press Release: Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy, available at: https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles

[27] Federal Trade Commission's Bureau of Consumer Protection (2018) *The Internet of Things and Consumer Product Hazards*. Available at: https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-federal-trade-commissions-bureau-consumer-protection-consumer-product-safety/p185404_ftc_staff_comment_to_the_consumer_product_safety_commission.pdf

[28] "In its case against BLU Products, the FTC alleged that a mobile device manufacturer had violated Section 5 of the FTC Act by failing to maintain reasonable security when, among other things, it failed to exercise oversight of its service provider. In part, the FTC alleged that the company did not even put in place basic contractual provisions requiring its service providers to maintain" pg. 7, FTC Testimony to CPSC.

[29] National Conference of State Legislates (2018) *State Laws Related to Internet Privacy.* Available at: http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx

Four states- California[30], Connecticut[31], Delaware[32], and Nevada[33]- have passed law requiring certain organisations to provide policy notices. California[34] and Utah[35] require all non-financial businesses to disclose to customers, via post or email, the types of personal information the business shares with or sells to a third party for direct marketing purposes or for compensation. In the area of "connective devices," California has a law in place that requires manufacturers to ensure that users of internet-connected televisions are prominently informed that their voices may be recorded and transmitted back to the manufacturers or third-party providers. The law also prohibits manufacturers from using or selling voice recordings for advertising purposes.[36]

Notably, data breach legislation exists in all 50 states. Massachusetts implemented information security regulations applying to any person who owns or licenses personal information about a resident of Massachusetts.[37] The regulations require that personal information be encrypted when stored on portable devices, or transmitted wirelessly or on public networks. The regulation also require the implementation of a comprehensive information security program.[38]

The state legislation with the broadest scope and most significant impact is the June 28, 2018 *California Consumer Privacy Act of 2018*, which generally applies to any business meeting the following conditions as stated in the law:

> (A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.
>
> (B) Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.
>
> (C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.[39]

The definition of personal information in the law is information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[40] The law provides that civil penalties for violations ivil action

---

[30] California Legislative Information (2003) *C 22. Internet Privacy Requirements [22575 - 22579]* Available at: http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=BPC&division=8.&title=&part=&chapter=22.&article=

[31] JUSTIA (2011) *Gen. Stat. § 42-471.* Available at: https://law.justia.com/codes/connecticut/2011/title42/chap743dd/Sec42-471.html

[32] State of Delaware (2016) *Chapter 12*. Available at: http://delcode.delaware.gov/title6/c012c/index.shtml

[33] NELIS (2018) S.B. 538 .Available at: https://www.leg.state.nv.us/App/NELIS/REL/79th2017/Bill/5818/Text

[34] California Legislative Information (2003) *California Civil Code §§ 1798.83 to .84 ("Shine the Light Law")*. Available at: http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.83.

[35] Utah State Legislature (2003*) Utah Code §§ 13-37-201 to -203.* Available at: https://le.utah.gov/xcode/Title13/Chapter37/13-37-P2.html?v=C13-37-P2_1800010118000101

[36] California Legislative Information (2015) *AB-1116 Connected televisions*. Available at: https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201520160AB1116

[37] 201 CMR: OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION: 17.02:
Personal Information, a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident:
(a) Social Security number;
(b) driver's license number or state-issued identification card number; or
(c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

[38] Office of Consumer Affairs and Business Regulation (2017) *Standards for the Protection of Personal Information of Residents of the* Commonwealth. Available at: https://www.mass.gov/files/documents/2017/10/02/201cmr17.pdf

[39] See section 1798.140 (c), available at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

[40] See section 1798.140 (o), available at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

brought by the California Attorney General to pay penalties up to 7,500 USD per intentional violations, and up to 2,500 USD for unintentional violations (if not remedied within 30 days).

In cases of certain data security breaches, consumers may institute civil actions to recover damages in an amount not less than $100 and not greater than $750 per consumer, per incident, or actual damages, whichever is greater.

Department of Commerce

The U.S. Department of Commerce (DOC) has also engaged in the issue of IoT privacy. Both the National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration (NTIA) (both agencies are part of the DOC) have engaged in this area.

Between 2016 and 2018, NTIA published a green paper on "*Fostering the Advancement of the Internet of Things*"[41], and convened a number of multi-stakeholder meetings to discuss various aspects of IoT security.[42] In July 2018, NIST convened a workshop on "*Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*".[43] The pre-read document for the workshop includes a table of "NIST SP 800-53 Controls Affected by IoT Privacy Risk Considerations", which includes a list of possible privacy challenges in the IoT environment, and suggests example of compensating controls. NIST SP 800-53 is a list of security and privacy controls for Federal Information Systems and Organisations; the list of controls applies to the Federal government. In September 2018, NIST announced plans to collaboratively develop a Privacy Framework intended as a "voluntary, enterprise-level tool that could provide a catalogue of privacy outcomes and approaches to help organisations prioritise strategies that create flexible and effective privacy protection solutions, and enable individuals to enjoy the benefits of innovative technologies with greater confidence and trust."[44]

[41] The Department Of Commerce Internet Policy Task Force & Digital Economy Leadership Team (2017) *Fostering the Advancement of the Internet of Things.* Available at: https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf
[42] National Telecommunications and Information Administration (2018) *Internet Policy, Internet of Things.* Available at: https://www.ntia.doc.gov/category/internet-things
[43] National Institute of Standards and Technology (2018*) Pre-Read Document for the NIST Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks Workshop.* Available at: https://www.nist.gov/sites/default/files/documents/2018/06/28/draft-iot-workshop-pre-read-document.pdf
[44] National Institute of Standards and Technology (2018) NIST Privacy Framework. Available at: https://www.nist.gov/sites/default/files/documents/2018/09/04/privacyframeworkfactsheet-sept2018.pdf

4.3 Japan

Japan has become a global driver of the IoT ecosystem, particularly in the robotics industry. IoT is projected to add nearly 960 billion USD to Japan's GDP in the next 15 years, under current conditions. Japan initially implemented a privacy law- the *Act on the Protection of Personal Information (APPI)* in 2003, and the law was fully enforced in 2005.[45] Amendments to the law came into force in January 2016, while other amendments came into force on 30 May 2017. The Amendment Laws to the APPI[46]:

- Define, expand and strengthen protection of "personal information"
- Introduce new requirements for anonymised (or "de-identified" information, and accompanying report to serve as a reference on anonymisation[47]
- Establish the Personal Information Protection Commission (PPC) (2016) dedicated to the establishment and enforcement of privacy regulations.
- Introduce new legislation on data transfers: the law restricts data transfers to a third country without obtaining data subjects' consent, unless the recipient country:
    1) Is specified in a PPC Ordinance as a country having a data protection regime equivalent to that of Japan (such as the EU- see below); or
    2) The third party recipient has a system of data protection that meets the standards prescribed by the PPC Ordinance; or
    3) The recipient has been certified under an international framework (such as the APEC Cross Border Privacy Rules), recognised by the PPC, regarding its system of handling personal information.

- Extraterritorial application of the APPI to entities outside of Japan if they receive personal information in connection with the provision of goods or services to individuals residing in Japan.

In July 2018, after a consultation process initiated in January 2017, the European Commission announced that Japan and the European Union will formally recognise each other's data protection systems as providing an equivalent level of protection for consumers in both markets.[48]

[45] Government of Japan (2013) *Act on the Protection of Personal Information.* Available at: http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf
[46] Personal Information Protection Commission (2018) *List of Laws and Policies*. Available at: https://www.ppc.go.jp/en/legal/
[47] Personal Information Protection Commission Secretariat (2017) *Anonymously Processed Information.* Available at: https://www.ppc.go.jp/files/pdf/The_PPC_Secretariat_Report_on_Anonymously_Processed_Information.pdf
[48] Paul Ulrich (2017) *The GSMA welcomes agreement by the EU and Japan on cross-border data flows.* Available at: https://www.gsma.com/publicpolicy/the-gsma-welcomes-agreement-by-the-eu-and-japan-on-cross-border-data-flows

4.4 India

Supreme Court Judgment on Privacy (2017)

In August 2017, the Supreme Court (SC) of India ruled privacy as a fundamental right. Delivered unanimously by a nine Judge Constitution bench, it also touched upon the aspects of informational privacy: digital age/footprint, use of data etc. Some relevant excerpts from the Judgment as below:

"*Data mining processes together with knowledge discovery can be combined to create facts about individuals. Metadata and the internet of things have the ability to redefine human existence in ways which are yet fully to be perceived…"*

"…Digital platforms are a vital tool of ensuring good governance in a social welfare state. Information Technology – legitimately deployed is a powerful enabler in the spread of innovation and knowledge."

"…These digital footprints and extensive data can be analysed computationally to reveal patterns, trends, and associations, especially relating to human behaviour and interactions and hence, is valuable information. This is the age of 'big data'."

"…The technological development today can enable not only the state, but also big corporations and private entities to be the 'big brother'…"

"…formulation of data protection is a complex exercise which needs to be undertaken by the state after a careful balancing of privacy concerns and legitimate State interests, including public benefit arising from scientific and historical research based on data collected and processed…"

"Since the government has initiated the process of reviewing the entire area of data protection, it would be appropriate to leave the matter for expert determination so that a robust regime for the protection of data is put into place. We expect that the Union government shall follow up on its decision by taking all necessary and proper steps."

The draft "Personal Data Protection Bill 2018" of J. Shrikrishna Committee

The Indian government in July 2017 constituted a Committee of Experts[49], chaired by Justice B N Shrikrishna, to work on a data protection framework and a draft bill for India. The objective was to "*ensure growth of the digital economy while keeping personal data of citizens secure and* protected."

The Committee released a white paper on "Data Protection Framework for India"50 listing down seven key principles namely. Technology agnosticism, Holistic application, Informed consent, data

[49] Ministry of Electronics & Information Technology (2017) Constitution of a Committee of Experts to deliberate on a data protection framework for India. Available at: http://meity.gov.in/writereaddata/files/meity_om_constitution_of_expert_committee_31072017.pdf

[50] Ministry of Electronics and Information Technology (2017) *White Paper of the Committee of Experts on a Data Protection Framework for India.* Available at: https://innovate.mygov.in/wp-content/uploads/2017/11/Final_Draft_White_Paper_on_Data_Protection_in_India.pdf

minimisation, controller accountability, structured enforcement, deterrent penalties. While envisaging challenges and new approach it will have to take due to emerging technologies, it said:

"*…Since technologies such as Big Data, the Internet of Things and Artificial Intelligence are here to stay and hold out the promise of welfare and innovation, India will have to develop a data protection law which can successfully address the issues relating to these technologies, so as to ensure a balance between innovation and privacy. Whether this involves a reiteration of traditional privacy principles, an alternative approach based on newer ex ante forms of regulation or a hybrid model, will have to be determined carefully…"*

The Committee recently released its report[51] on the whitepaper along-with a *draft* Personal Data Protection Bill 2018[52]. The bill seems influenced by GDPR e.g. a consent-centric framework, cross border data flows, heavy penalties for data breaches, proposing establishing a separate Data Protection Authority (DPA) among others. Some key features of the draft bill are as follows:

- Applicability / Jurisdiction: both government and private entities are covered and it extends not only to processing of personal data by Indian entities but also to foreign entities that collect and process personal data for offering goods or services or for profiling individuals within India.
- Data Protection obligations for processing of personal data – the bill makes some obligations on any person processing personal data of any individual (also termed as a "Data Principal"). These are *fair and reasonable processing*, *purpose limitation, collection limitation, lawful processing, notice, data quality, storage limitation, and accountability*.
- Data Principal: natural person to whom personal data (defined at sub-clause 28 of definition) relates
- Data Fiduciary: an entity or an individual who determines the purpose and means of processing of personal data of the "data principal" is termed as a "data fiduciary".
- Significant data fiduciary: to be notified by the data protection authority based on parameters such as sensitivity of personal data, volume of personal data processed by the data fiduciary, turnover of the data fiduciary, risk of harm etc.; and, such entity would be subjected to heightened scrutiny.
- Types of Personal Data: There are three different categories[53] of personal data that are indicated in the draft bill i.e. Personal Data, Sensitive Personal Data and Critical Personal Data. *Anonymized data* is not considered personal data and thus is not covered. The definition of "personal data" now rests on the criterion of whatever makes an individual identifiable. The definition of sensitive personal data has been expanded.
- Basis for Processing: There are several different grounds for legal processing of data at the core of which is the consent framework which remains the primary basis to collect and process all types of personal data and it should be: (a) free, (b) informed, (c) specific; (d) clear and (e) capable of being withdrawn. For the narrower category of "sensitive personal data" explicit consent is mandated.

---

[51] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018) *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians.* Available at: http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf

[52] Ministry of Electronics & Information Technology (2018) *the Personal Data Protection Bill, 2018.* Available at: http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf

[53] **Personal Data**: "...*data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identify of such natural person, or any combination of such features, or any combination of such features with any other information*…" (Chapter I Section 29).
Sensitive personal data: "…*personal data revealing, related to, or constituting… (I) passwords; (ii) financial data; (iii) health data; (iv) official identifier; (v) sex life; (vi) sexual orientation; (vii) biometric data; (viii) genetic data; (ix) transgender status; (x) intersex status; (xi) caste or tribe; (xii) religious or political belief or affiliation*…" (Chapter I Section 35). The DPA can notify other characteristics considered sensitive.
Critical personal data: Only that data deemed critical shall be notified by the government and may only be processed on servers located in India.

Other grounds are Prompt action (e.g. medical emergency or disaster situation), employment-related purpose of an employee and reasonable purposes (to be specified by the DPA).

- Localization and Cross-Border Transfers: The chapter VIII of the draft bill covers the system governing cross-border transfers of personal data, which seems complex in the present form.
- Some cross border transfers of personal data that may include sensitive personal data – is allowed under standard contracts, approved intra-group schemes or a country-by-country adequacy determination by the government. A class of "critical personal data" considered so strategic that the government will notify has been created and this data cannot be transferred out and will have to be processed only in India. A "serving copy" of all types of personal data must be held in India.
- The government may exempt specific categories of non-sensitive personal data from mirroring requirements on the basis of "necessity or strategic interests of the state."
- User Rights: The draft Personal Data Protection Bill grants some specific rights to data principals, including, Confirmation and Access, Correction, Data portability, Right to be forgotten
- Administration and Fines: The draft proposes creation of a Data Protection Authority (DPA) to "*protect the interests of data principals*" and cover other aspects like ensuring compliance etc. The DPA could levy fines potentially reaching 4% of global turnover of companies in cases of violations.
- Data fiduciaries would also be required to notify the DPA in response to a breach that is "*likely to cause harm to any data principal.*"
- The committee has refrained from imposing a typical GDPR style law with a broad brush in India and as a result, it has both narrowed its applicability (e.g. exempting small manual processors or onerous requirements for specially notified classes of data fiduciaries) and relaxed some standards (e.g. right to be forgotten and breach notification obligations). Further, the eventual DPA will define the acceptable codes of practices.

TRAI Recommendations on 'Privacy, Security and Ownership of the Data in the telecom sector':

- The Indian Telecom Regulator TRAI, to bring out the multiple aspects of the data protection in the telecom sector and to identify key issues pertaining to data protection in relation to the delivery of digital services through the telecom systems, issued a consultation paper[54] on "Privacy, Security and Ownership of the Data in the telecom sector" issued[55] its recommendations on the same. While making some pertinent observations, TRAI broadly recommended the following:

Data and its ownership:

1. It is the user who owns his/ her personal information/ data collected by/ stored with the entities in the digital ecosystem.
2. The entities, controlling and processing such data, are mere custodians and do not have primary rights over this data.

[54] Telecom Regulatory Authority of India (2017) *Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector.* Available at: https://trai.gov.in/sites/default/files/Consultation_Paper%20_on_Privacy_Security_ownership_of_data_09082017.pdf

[55] Telecom Regulatory Authority of India (2018) *Recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector.* Available at: https://trai.gov.in/sites/default/files/RecommendationDataPrivacy16072018.pdf

3. Anonymisation– TRAI feels certain standards for anonymisation/de-identification of data are required, which can be determined after undertaking some studies.
4. Metadata - Since in certain cases metadata can be used by the entities operating in the digital eco-system to identify the individual users, such entities must be restrained from using metadata to identify the users/individuals.

Personal Data (PD) and framework:

1. Personal Data – the current definition of PD as defined under the Information Tech (IT) Act is fine but the existing framework for protection of such data is not sufficient. Therefore
    a. To protect consumers against misuse of their PD by the broad range of data controllers and processors in the digital ecosystem, all entities in the digital ecosystem, which control or process their PD should be brought under a data protection framework.
    b. Till such time a general Data protection law is enacted the existing Rules/ License conditions applicable to MNOs for protection of users' privacy be made applicable to all the entities in the digital ecosystem.
    c. Devices manufacturers should disclose T&Cs of use in advance, before device sale.

Consent, Choice, Data Portability:

2. Telecom consumers should have the Right to - Choice, Notice, Consent, Data Portability, and, to be Forgotten
3. Data Controllers should be prohibited from using "pre-ticked boxes" to gain users consent.
4. All entities in the digital ecosystem should transparently disclose the information about the privacy breaches on their websites along with the actions taken
5. A common platform should be created for sharing of information relating to data security breach incidences by all entities in the digital ecosystem including MNOs.

Issues like cross border data flow, regulatory sandboxes, data controllers and processers – while commented upon by TRAI, it refrained from making any recommendations.

Legislative Proposal

The Justice Shrikrishna Committee of Experts has published a draft Personal Data Protection Bill 2018[56] and the government has now sought feedback[57] from public (by 10th September 2018) on this draft bill. Subsequently bill will go through multiple stages before the Parliament enacts it into a law (e.g. approval of the Union Cabinet and then presenting it in the Parliament for discussion and debate).

Currently applicable definitions from other sources

In terms of the legislative norms applicable currently, India has the Information Technology Act 2000 and the Information Technology (Reasonable security practices and procedures and

[56] Ministry of Electronics & Information Technology (2018) *the Personal Data Protection Bill, 2018.* Available at: http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf
[57] Ministry of Electronics & Information Technology (2018) *Public given 10 more days to give views on Draft Personal Data Protection Bill.* Available at: http://meity.gov.in/writereaddata/files/Submission_date_10.10.2018.pdf

sensitive personal data or information) Rules 2011 (the ‘Reasonable Security Practices Rules’) issued under the IT Act. Under these rules:

(a) "**Data"** – defined in section 2(1)(o) of the IT Act, 2000 as a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

(b) **"Information**"– defined in section 2(1)(v) of the IT Act,2000 as a term including data, text, images, sound, voice, codes, computer programs, software and databases or micro film or computer generated micro fiche.

(c) "**Personal information**"– defined in the SPDI Rules, 2011 as any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

(d) "**Sensitive personal data or information**"– defined in the SPDI Rules, 2011 as such personal information which consists of information relating to:- password, financial information such as bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; biometric information; any detail relating to the above clauses as provided to body corporate for providing service; and any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise; provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

The draft Personal Data Protection Bill 2018 also proposes some amendments in the IT Act, to make certain definitions in that in line with the new definitions proposed.

Telecom Regulations / License Conditions

Further, the MNOs being the Telecom licensees in India, are subject to some exhaustive obligations that cover aspects of user information and its sharing (restrictive). There are a number of applicable legislation and policies that contain provisions with a bearing on the right to privacy and data security in the telecom sector in India e.g.:

- IT Act, 2000, and IT rules: Sec 43A, Sec 69, Sec 69B, Sec 72A, Sec 67C, and Sec 79
- Indian Telegraph Act, 1885: Sec 5 and Sec 26,
- Indian Telegraph Rule 419A
- Unified License conditions 37, 38, 39 and 40
- Guidelines, circulars, direction, and notifications issued by DoT and TRAI from time to time

4.5 Brazil

Brazil is striving to become a global player in the IoT arena. The country's first move in this direction dates back to 2012, when a presidential decree established an 80% reduction of one of the telecom-specific taxes levied on connections and paid by MNOs. In practice, this was only implemented in 2014, with the publishing of a directive from the Ministry of Communications that defined M2M and created a management chamber for M2M that would be composed of representatives of several government bodies as well as from the private sector and research institutions.

In the field of privacy, Brazil lags behind even its Latin American neighbours. While privacy is mentioned in a few different laws (such as the Consumer Code and the Civil Rights Framework for the Internet), the country still lacks a comprehensive privacy law. In June 2018, Congress approved a draft privacy bill after almost eight years of back-and-forth between the various instances in the Executive and in Congress. At of the time of writing this document, the bill had not yet been sanctioned by the President.

This bill, if approved, would determine important definitions, safeguards, and restrictions regarding the use of data, including:

- Define what is "personal information", the principles that should govern its protection, and the alternatives that allow its collection and processing;
- Defines what is "anonymised data", creates the right of users to request anonymisation, and exempts data that has been anonymised (and cannot be de-anonymised by reasonable means) from the law;
- Creates the right of users to request data portability;
- Creates the right of users to request a re-evaluation of decisions based entirely on the automated processing of personal data;
- Establishes the extraterritorial element of the law, which means that data collected in Brazil and/or processing is aimed at offering services for individuals located in Brazil would place the operation under the scope of the law;
- Establishes rules for international data transfers;
- Establishes a National Data Protection Authority (DPA), although this has yet to be defined by the Presidency.

5. Considerations for Applying Privacy Principles to IoT

Most privacy frameworks, including legislation and self-regulatory initiatives, are based on the same set of global privacy principles[58]. These principles are reflected in the *GSMA Mobile Privacy Principles*[59] which describe the way in which mobile consumers' privacy should be respected and protected when they use mobile applications and services that access, use or collect their personal data.

The principles do not replace or supersede applicable law, but are based on recognised and internationally accepted standards on privacy and data protection. They seek to strike a balance between protecting an individual's privacy and ensuring they are treated fairly while enabling organisations to achieve commercial, public policy and societal goals. Generally speaking, they are flexible enough to accommodate new technologies and business methods as they arise.

Widely accepted privacy principles can be applied to the IoT to protect individuals without the need for sector-specific legislation, however, device manufacturers, service providers, and other players in the IoT ecosystem should be aware of the IoT-specific privacy considerations.

[58] GSMA (2017) *Cross-border data flows.* Available at: https://www.gsma.com/publicpolicy/wp-content/uploads/2017/10/GSMA-Cross-Border-Data-Flows_4pp_2017_WEB.pdf
[59] GSMA (2016). *Mobile Privacy Principles*. Available at: https://www.gsma.com/publicpolicy/wp-content/uploads/2016/02/GSMA2016_Guidelines_Mobile_Privacy_Principles.pdf

Areas requiring special attention

Addressing specific IoT and big data privacy requirements remains a non-trivial challenge. We identify below three specific areas that require special attention and illustrate them with examples.

1) When IoT data is considered "personal"?

Example: Smart Bin

An IoT device monitors how full a garbage bin is. The sensor inside the bin is able to measure the amount of garbage inside and communicate it to the utility company on a regular basis (daily or even more frequently). The garbage bin is located right outside *a single house/ house block with a limited number of households*. The utility company collects data from the bin to optimise the collection process. The collection truck will only collect garbage when the bin is sufficiently full.

While the amount of litter in the bin may not be regarded as a private information, when this is used in conjunction with contextual information about the bin location, it could be used to detect specific behaviours of the households closer the bin. For example, it may indicate whether people are currently living in the nearby houses and how much litter is being produced could be used to estimate how many people are living there.

While implementing the service it important to consider a number of relevant questions:

a) *Does the service collect information that can, directly or indirectly identify a specific user?*
"Location data" is intended as information that identifies the geographical location of a user which may include Cell ID, GPS, Wi-Fi or even other less granular information such a street name. To be identified, an individual need not be known by name. Assess the level of granularity of information (location of bin and garbage level in the bin) against the possibility of the individual/s to be traced back through applications correlating households and bin location.

b) *How data will be used?*
Will data only be used for identifying the optimal route or for other purposes? For example, is the utility company considering introducing a pay-per-use charging systems where residents will be charged on the amount of garbage produced? This may be a perfectly reasonable use of the data, only it will require appropriate transparency and user consent.

c) *Will data be permanently stored and if not how long will it be kept for?*
Is there a need to keep historical records of data? If so, what are the purposes? Best practice requires personal information to be kept only for the time necessary for those legitimate business purposes it has been collected for or to meet legal obligations and should subsequently be deleted or rendered anonymous. In the example, there may be various legitimate purposes for storing data longer than the simple garbage collection, for example data could be used for local infrastructure planning, reporting again government targets or for the utility company resource planning.

d) *Will data be shared with third parties? Who are they and for what reason do they access data?*

For example, is the utility company considering sharing data with the local council? The council may want to legitimately use anonymised data to assess local rates or delivery of other local services. Or is data used to identify specific behaviours, for example the Council may want to establish whether people actually and currently live in specific households nearby. Other commercial businesses may be interested in what products people use. A local pizza delivery company, or a supermarket chain may be interested in how residents behave from the amount of garbage produced particularly in areas subject to seasonal residency.

2) Who is the "data controller"?

Example: Smart Tractor

An agriculture tractor has IoT sensors which detect data such as soil humidity and composition, level of hydration of crops, pesticides and fertilizer administered in specific field locations. The service is provided by the tractor manufacturer, and a mobile network operator is providing connectivity service to the tractor manufacturer. Data recorded on the field is stored on the service provider database. The tractor manufacturer performs analytics on data collected to improve tractor performance, conduct 'real-time' application of products such as pesticides as needed on crops and monitor efficiency of its services. The owner of the tractor can access data related to its own fields/crop through a portal that the tractor manufacturer makes available, using data generated transmitted via the mobile network services.

In this example, the data involved can be both personal and non-personal, and there may be confidentiality obligations for both the tractor manufacturer and the service provider. Those obligations may be established in the law or through legal agreements. Data protection obligations would only apply to any personal data e.g., the personal data relating to the farmer. In the example, the tractor manufacturer is a data controller for any personal data. For example, if the tractor manufacturer collects data related to the location and movements of the tractor, this could constitute personal data along with information such as the name and address of the farmer.[60]

However, other types of data collected from the end-user or determined from the IoT devices may need to remain confidential, despite being non-personal. Soil humidity, location, timing and quantify of fertilizer administered may constitute commercially sensitive data for the farmer. For example, he/ she may consider this confidential information that may gain competitive edge on nearby producers, or even companies interested in futures markets for agricultural commodities.

Given that there are both confidentiality and data protection obligations to consider, it is helpful to identify the responsibilities of the different players in the ecosystem. For example, in this case, the tractor manufacturer is offering a service to consumers and is retaining data for analytics. The tractor manufacturer would be the data controller responsible for handling personal data. The consumer in this case may be an individual, or it may be a commercial farm. The tractor manufacturer may subcontract certain services e.g., systems development or hosting to third parties. The tractor manufacturer, in assuming the role of data controller for its own customers should consider a number of relevant questions:

[60] As the previous example, this one too is useful to understand how data not considered personal can indeed become personal. If there is only one user of the tractor, the tractor remains in the same geographic area where few farmers, whose identities can be publicly known, grow a specific crop, then the crop data could become personal data. If the tractor manufacturer partners with another company to conduct research on energy expenditures based on types of crops, and this data is released, then anyone with access to the names of farmers growing specific crops can be paired with the energy data organised by crop type, thereby revealing a farmer's energy use.

- Is the consumer a natural person or a legal person?
- If a legal person owns the tractor, is there a legal basis in place to collect personal data from the user of the tractor? (e.g., does the manufacturer also need to obtain consent from the user to track location data?)
- Which other organisations or persons are acting as a processor for the tractor manufacturer? If so, what kind of agreements are in place regarding data handling?
- Is the mobile network operator providing pure connectivity services or are they providing other information such as data analytics that are used by the tractor manufacturer to support the smart tractor service?
- Does the jurisdiction have data subject rights in place, such as data portability, access, correction, or deletion (as in the GDPR)?
- Which data should be included in a portability request? Is this limited to data the service provider collected from the farmer in order to use the service, or does that also include the data generated by the tractor and its sensors?
- What are the confidentiality obligations for the tractor manufacturer or for the mobile network operator? Are these subject to a law, or to a contractual agreement, or both?

These represent some key issues associated with the respective data protection and confidentiality responsibilities of different ecosystem players. The GSMA has covered key security considerations in the *IoT Security Guidelines*.[61]

[61] GSMA (2016). *IoT security guidelines and assessment.* Available at: https://www.gsma.com/iot/iot-security/iot-security-guidelines/

3) Notice and Choice/Consent

Example: Smart Car: Pay-as-you drive insurance

An IoT device installed in a car, monitors the driving style of its driver: how fast he/she accelerates, whether he/she exceeds speed limits, what time of day is the car driven, and the total number of miles per day. The service also has an in-built cameras which, through facial recognition can detect which person is driving the car, and if the driver falls asleep to guarantee safe driving. The car's owner has signed up the privacy notice at the time of purchase and has been given transparent access to all documentation. By accepting to disclose data with its insurance provider he/she can save on the annual premium if he is profiled a 'good' driver. However, the driver's partner occasionally drives the car too. He/she is being recorded and, in conjunction, her driving styles is also being tracked.

In the example the person signing up to the IoT service is not the sole user of the service. He has been made aware of the personal data information being disclosed to the third party when he subscribed the service. However, the partner isn't. Designing services that provide the opportunity to give consent and that are transparent on which information is being recorded can be a challenge for some IoT devices.

In some instances devices do not have a screen, and information cannot be presented and agreed upon by the end user. Or if they have a screen, it may be impractical for the service functioning to have the user accepting privacy clauses every single time. Some of the users may find themselves disclosing personal data, such as in this case driving habits, personal location at a moment in time, or video footage, without having expressed consent.

Auto manufacturers are well aware of these use cases, they are increasingly common as technology advances and some of these services are being sold as after-market devices. These are stand-alone "sat-navs" or cameras that can be installed in the car by the end-user. In this case the service provider will be the sat-nav or camera provider. The end-user by purchasing and installing the device will agree to separate terms and conditions.

The example above should be considered only for illustrative purposes. While designing the service a number of questions should be considered:

a) How do you provide notice and obtain consent in situations where:
   a. There may be passive collection of data
   b. There may not be a screen on which to present a notice or a companion application
   c. There may not be a first-person, direct relationship with the individual

6. Annex

Summary of IoT Privacy and Summary Principles Identified in Report on Workshop on Security & Privacy in IoT / 13 January 2017

Wearables and Smart Appliances

Top seven minimum baseline security and privacy principles identified at the workshop:

1. Data control by the user – in any phase of the data life cycle and product life cycle

2. Transparency and user interface control – empower the user to obtain sufficient knowledge on what its devices and related system are doing and sharing, even if it concerns M2M communications and transactions

3. Encryption by default – in communication, storage and otherwise

4. Relatively high level of baseline – when safety is at stake, or critical infrastructure or national safely can be materially impacted

5. Lifetime Protection – give security, safety and privacy protection over the full life time

6. Updatability – trusted and transparent updates only by authorised parties, not by malicious actors

7. Identity protection by design – decoupling personal identity from device identity

Connected and Autonomous Vehicles

Top five minimum baseline privacy principles in IoT identified at the workshop, in no particular order

1. Data segmentation, also within the domain of personal data – as per the context of the personal data, the multiple personae each data subject has, and the related protection – including fundamental and consumer rights – it has

2. Data control, assess and use to be defined – as per the various stakeholders, such as drivers, passengers, vehicle owner, peer-to-peer sharing persons, manufacturers, service providers and so forth

3. Transparency as primary requirement – awareness, informed and unambiguous consent per contextual processing of personal data (which data for which use)

4. User control – choice of the user: possibility to opt-out, data subject right to access their data and portability right of their data, communication platform to control data access and to ensure security and privacy, and the overall securing of personal data processed, not only in and by the vehicle, but also in the context of related systems and devices (e.g. navigation-satellite)

5. Privacy by design and privacy by default – earmarking data collection, ensure data minimisation, and the ability to hold liable the manufacturer or service provided for misuse of collected personal data

Top five security principles identified, in no particular order:

1. Harmonised industry approach – standardisation of the functional and security assurance requirements through common harmonised industry approach: 1) in which every control unit is to be protected and 2) connectivity unit such as vehicle information control and access control) to benefit from a higher protection

2. Harmonisation approach – reduce the impact of different national regulations

3. Updatability and upgradability ("security as a moving target") – use of related securitisation processes with 1) need for regular updates and upgrades during the vehicle lifetime, and 2) need to use identifiers for an adequate identification of devices

4. End of support – where the current practice is about 12 to 15 years, the end of life cycle and the related support is prerequisite. Questions to be addressed are: what happens if a services agreement is lawfully terminated, is there an update possibility, when will updating and upgrading become limited, and who is accountable for the risk of not updating IoT devices and systems

5. Identifying and securing interface points – also to reduce the risk of security breach

Industrial IoT

Regarding privacy, the group noted that both the legal frameworks and respective requirements arising Maria Gorjainovag out of the GDPR as well as the ePrivacy directive/regulation where identified as baseline privacy and security requirements.

Smart Cities

The top eight minimum baseline security and privacy requirements that surfaced in this breakout session:

1. Human-centric – security and privacy should be universally applied to data subjects

2. Data isolation – functional separation of datasets and databases

3. Transparent roles – ensuring clear allocation and identification of roles, including who is data controller, co-controller, processor, co-processor, and so forth

4. Single point of contact – provide single point of contact for personal data protection and privacy

5. Non-discriminatory practices – ensure non-discriminatory practices against data subjects (citizen and any other persona such individual may have while being part of the ecosystems of a city) and businesses on the basis of information derived from IoT deployments within smart cities

6. Independent privacy and security audits – cities of a certain size should mandatorily carry out thirds party privacy and security audits

7. Dynamic trust KPIs and metrics – on security, privacy, safety, resilience, reliability and the like

8. Continuous monitoring – ensure continuous monitoring and improvement of IoT ecosystems, including clear metrics and measurements

7. References

Global

1. GSMA (2016). *Mobile Privacy Principles*. Available at: https://www.gsma.com/publicpolicy/wp-content/uploads/2016/02/GSMA2016_Guidelines_Mobile_Privacy_Principles.pdf

59. GSMA (2017) *Cross-border data flows.* Available at: https://www.gsma.com/publicpolicy/wp-content/uploads/2017/10/GSMA-Cross-Border-Data-Flows_4pp_2017_WEB.pdf

58. GSMA (2016). *Mobile Privacy Principles*. Available at: https://www.gsma.com/publicpolicy/wp-content/uploads/2016/02/GSMA2016_Guidelines_Mobile_Privacy_Principles.pdf

61. GSMA (2016). *IoT security guidelines and assessment.* Available at: https://www.gsma.com/iot/iot-security/iot-security-guidelines/

Europe

5. EC (2018). *Article 29 Working Party Guidelines on consent under Regulation 2016/679.* Available at: http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030

6. GSMA (2012*) Privacy Design Guidelines for Mobile Application Development*. Available at: https://www.gsma.com/publicpolicy/privacy-design-guidelines-mobile-application-development

7. EC (2017*) Proposal for a Regulation of the European Parliament and of the Council*. Available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241

8. The European Parliament and the Council of the European Union (2016) *The EU General Data Protection Regulation, article 13.* Available at https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A13

9. Hogan Lovells (2017) *Draft e-Privacy Regulation End users' terminal equipment rules*. Available at: https://www.hldataprotection.com/files/2017/01/Draft-e-Privacy-Regulation-End-users-terminal-equipment-rules.pdf

10. BEREC (2016) *Report on Enabling the Internet of Things*, page 21. Available at: https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/5755-berec-report-on-enabling-the-internet-of_0.pdf

11. Council of the European Union (2018) *Document 10975/18*. Available at: https://iapp.org/media/pdf/resource_center/ePR-draft-July-2018.pdf

13. EC (2017) *Report on Workshop on Security & Privacy in IoT, Annex 1.* Available at: http://ec.europa.eu/information_society/newsroom/image/document/2017-15/final_report_20170113_v0_1_clean_778231E0-BC8E-B21F-18089F746A650D4D_44113.pdf

15. EC (2014) *Article 29 Working Party Opinion 8/2014 on the on Recent Developments on the Internet of Things.* Available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

16. EC (2013) *Opinion 02/2013 on apps on smart devices.* Available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

USA

18. T John Eggerton (2018) Ninth Circuit Clarifies: FTC Common Carrier Carve-Out Is Activity Based. Available at: https://www.broadcastingcable.com/news/ninth-circuit-clarifies-ftc-common-carrier-carve-out-activity-based-172046

19. Legal Information Institute (2017) *Customer Proprietary Network Information regulation*: https://www.law.cornell.edu/cfr/text/47/part-64/subpart-U

20. Federal Trade Commission (2018) *Privacy and Security Enforcement, Press Releases.* Available at: https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises

21. Federal Trade Commission (2017) *VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent.* Available at: https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it

22. Federal Trade Commission event page (2013*): Internet of Things - Privacy and Security in a Connected World* workshop, available at: https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world

23. Federal Trade Commission (2015) *Internet of Things Privacy & Security in Connected World.* Available at: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

24. Federal Trade Commission (2017) Press Release: *FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras*, available at: https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate

25. Federal Trade Commission (2016) Press Release: *ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk*, available at: https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put

26. Federal Trade Commission (2013) Press Release: Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy, available at: https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles

27. Federal Trade Commission's Bureau of Consumer Protection (2018) *The Internet of Things and Consumer Product Hazards*. Available at: https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-federal-trade-commissions-bureau-consumer-protection-consumer-product-safety/p185404_ftc_staff_comment_to_the_consumer_product_safety_commission.pdf

29. National Conference of State Legislates (2018) *State Laws Related to Internet Privacy.* Available at: http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx

30. California Legislative Information (2003) *C 22. Internet Privacy Requirements [22575 - 22579]* Available at: http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=BPC&division=8.&title=&part=&chapter=22.&article=

31. JUSTIA (2011) *Gen. Stat. § 42-471.* Available at: https://law.justia.com/codes/connecticut/2011/title42/chap743dd/Sec42-471.html

32. State of Delaware (2016) *Chapter 12*. Available at: http://delcode.delaware.gov/title6/c012c/index.shtml

33. NELIS (2018) S.B. 538 .Available at: https://www.leg.state.nv.us/App/NELIS/REL/79th2017/Bill/5818/Text

34. California Legislative Information (2003) *California Civil Code §§ 1798.83 to .84 ("Shine the Light Law")*. Available at: http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.83.

35. Utah State Legislature (2003*) Utah Code §§ 13-37-201 to -203.* Available at: https://le.utah.gov/xcode/Title13/Chapter37/13-37-P2.html?v=C13-37-P2_1800010118000101

36. California Legislative Information (2015) *AB-1116 Connected televisions*. Available at: https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201520160AB1116

38. Office of Consumer Affairs and Business Regulation (2017) *Standards for the Protection of Personal Information of Residents of the* Commonwealth. Available at: https://www.mass.gov/files/documents/2017/10/02/201cmr17.pdf

39. See section 1798.140 (c), available at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

40. See section 1798.140 (o), available at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

41. The Department Of Commerce Internet Policy Task Force & Digital Economy Leadership Team (2017) *Fostering the Advancement of the Internet of Things.* Available at: https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

42. National Telecommunications and Information Administration (2018) *Internet Policy, Internet of Things.* Available at: https://www.ntia.doc.gov/category/internet-things

43. National Institute of Standards and Technology (2018*) Pre-Read Document for the NIST Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks Workshop.* Available at: https://www.nist.gov/sites/default/files/documents/2018/06/28/draft-iot-workshop-pre-read-document.pdf

44. National Institute of Standards and Technology (2018) NIST Privacy Framework. Available at: https://www.nist.gov/sites/default/files/documents/2018/09/04/privacyframeworkfactsheet-sept2018.pdf

Japan

45. Government of Japan (2013) *Act on the Protection of Personal Information.* Available at: http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf

46. Personal Information Protection Commission (2018) *List of Laws and Policies*. Available at: https://www.ppc.go.jp/en/legal/

47. Personal Information Protection Commission Secretariat (2017) *Anonymously Processed Information.* Available at: https://www.ppc.go.jp/files/pdf/The_PPC_Secretariat_Report_on_Anonymously_Processed_Information.pdf

48. Paul Ulrich (2017) *The GSMA welcomes agreement by the EU and Japan on cross-border data flows.* Available at: https://www.gsma.com/publicpolicy/the-gsma-welcomes-agreement-by-the-eu-and-japan-on-cross-border-data-flows

India

49. Ministry of Electronics & Information Technology (2017) Constitution of a Committee of Experts to deliberate on a data protection framework for India. Available at: http://meity.gov.in/writereaddata/files/meity_om_constitution_of_expert_committee_31072017.pdf

50. Ministry of Electronics and Information Technology (2017) *White Paper of The Committee of Experts on A Data Protection Framework for India.* Available at: https://innovate.mygov.in/wp-content/uploads/2017/11/Final_Draft_White_Paper_on_Data_Protection_in_India.pdf

51. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018) *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians.* Available at: http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf

52. Ministry of Electronics & Information Technology (2018) *The Personal Data Protection Bill, 2018.* Available at: http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf

54. Telecom Regulatory Authority of India (2017) *Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector.* Available at: https://trai.gov.in/sites/default/files/Consultation_Paper%20_on_Privacy_Security_ownership_of_data_09082017.pdf

55. Telecom Regulatory Authority of India (2018) *Recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector.* Available at: https://trai.gov.in/sites/default/files/RecommendationDataPrivacy16072018.pdf

56. Ministry of Electronics & Information Technology (2018) *The Personal Data Protection Bill, 2018.* Available at: http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf

57. Ministry of Electronics & Information Technology (2018) Public given 10 more days to give views on Draft. Available at: http://meity.gov.in/writereaddata/files/Submission_date_10.10.2018.pdf

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at www.gsma.com. Follow the GSMA on Twitter: @GSMA.

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601