GSMA position

Background

The growth of the Internet and technological developments have led to an explosion of data created by, and about, consumers. 'Connected' and 'always on' devices and sensors are expected to boost this trend even more. The IoT offers significant opportunities and potential for data-driven innovation to achieve economic, social and public policy objectives and improve people's daily lives. For example, the IoT will enable a raft of new applications and services, empowering consumers to monitor their health, manage their energy consumption and generally benefit from 'smart' home and city solutions leading to lower pollution levels, better traffic management etc.

Many IoT services will be designed to create, collect or share data. Some of this data (for example, data about the physical state of the machines, environmental or weather conditions) may not be considered 'personal data' or impact a consumer's privacy, and therefore, not subject to data protection and privacy laws;

However, many IoT services will involve data about individual consumers and will be subject to general data protection and privacy laws. Where IoT services are provided by mobile operators they will also be subject to telecommunications-specific privacy and security rules. 'Consumer' IoT services are likely to involve the generation, distribution and use of detailed data that could impact on individuals' privacy. For example, from drawing inferences about their health to developing profiles based on their shopping habits and locations. As consumer IoT services gain in popularity, more consumer data will be created, analysed in real-time and shared between multiple parties across national borders.

Where data relates to specific individuals, this complex, 'connected' ecosystem may raise concerns over:

- Who is collecting, sharing and using individuals' data and why;
- How the security and privacy of individuals' information is ensured;
- The ability of individuals to exercise choice and control over how companies will use their data, especially when such use is unrelated to the original purpose for which it was collected.

Debate

- How can policymakers and industry partners ensure that potential data protection and privacy concerns are addressed in a way that strengthens – rather than hinders – the 'Internet of Things'?

Industry position

To realise the opportunities that the IoT offers, it is important that consumers trust the companies who are delivering IoT services and collecting data about them. The GSMA and its members believe that consumer confidence and trust can only be fully achieved when users feel their privacy is appropriately respected and protected.

There are already well-established data protection and privacy laws around the world which have applied to mobile operators for years. The GSMA believes that it is possible to apply existing data protection regulations and principles to address privacy needs in the context of IoT services and technologies.

However, IoT services typically involve more parties than simply mobile operators, such as device manufacturers, online platforms and even the public sector. It is important that there is regulatory clarity and legal certainty around IoT services and that privacy and data protection regulations apply consistently across all IoT providers in a service and technology-neutral way.

Regulators should support and encourage measures by which industry can identify and mitigate risks to privacy, and through which they can demonstrate accountability e.g. through privacy enhancing technologies and tools that help consumers to manage their privacy and control how their data are used.

The data protection and security practices developed for a given IoT service should reflect the overall risk to an individual's privacy and the context in which data about the individual is collected, distributed and used. Any regulatory interventions should be limited to areas where identified risks emerge and existing measures are insufficient to address these.

The GSMA and its members draw on their extensive experience in addressing privacy and security issues and work collaboratively with their IoT partners, such as device manufacturers, mHealth and mEducation service providers, to embed privacy and security into IoT technologies and the overall consumer experience. This on-going collaboration will ensure IoT industry partners are able to identify and mitigate the relevant consumer privacy risks in the context of the service being delivered.