Data Ownership and Privacy

What is it that entitles us to our rights to tangible assets? We all know that rights are inherently linked to the question of ownership. But, because of the intangible nature of data, how is its ownership determined which is central to determining who holds the rights over it? What are the challenges in protecting the individual's rights to personal data and the what provisions in privacy law protects such rights? Let's try and delve into more details.

The Vital Questions

In our daily lives, personal data is constantly being captured, whether by cookies on your computer, the CCTV camera at your bank, or by the fitness tracker that you wear. This could be either with or without our knowledge and permission, with potentially a huge bearing on our lives (fraud, identity theft, misuse, all come to mind).

The bulk of such data capture is a result of enterprises or institutions' (state or private) intent to make our, and their lives easier. The ordinary citizen has no choice but to give in and share their personal information or get locked out of the vast array of products and service offerings on offer today, either in the online or the physical market. So apparently, it is the willingness of both the consumer and the offeror of products or services that leads to capturing or generating of data pertaining to individuals.

The vital question then is, if data is generated for mutual benefit, who is its real owner? Below are two arguments that are contextual and thought provoking. Information security practice puts the onus of determining the confidentiality of an information asset on its author or creator. So, going by this logic, those who capture (or essentially create) data pertaining to

others' personal characteristics (e.g. a CCTV administrator capturing footage of individuals) should have ownership of such data (i.e. individual's CCTV footage). However, the individual, by whose physical existence and behavior, such data gets generated be construed as its real owner. How this has been addressed by privacy laws is discussed ahead.

So, what is Personal Data?

According to the European Union (EU) GDPR (General Data Protection Regulation), '**Personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Some further attributes of personal data are:

- It includes any type of statement about a person – objective (e.g. qualification) or subjective (e.g. work performance). Such Information doesn't need to be true to be considered as personal data.
- It includes any information regarding any activity (professional or public sphere) undertaken by the individual. The Court of Justice of European Union has established that the concept of private and family life should be widely interpreted. e.g. An individual's contact information at their place of work will be Personal data in the same way as their home address or phone number.
- Online identifiers such as an IP address, cookie or Radio Frequency (RF) tag may be used to create a person's profile and identify them and are therefore considered Personal data.

But where is your personal data?

A major challenge with data is that its capture, transmission and storage in electronic form poses lack of visibility to its owner about the temporal, locational and multiplicity of its persistence (e.g. in Cloud, offline backup tapes and data centres). As an example, your health tracker could be transferring your health data to cloud servers located in a country not covered by strong data protection and privacy laws and could therefore be vulnerable. The 2019 Data Breach Investigations Report by Verizon has quoted that personal information has been the most prevalent (close to 33%) amongst the types of data disclosed because of the data breaches.

Historically, concerns about misuse of personal data potentially leading to disadvantage to individuals was the main driving factor behind the evolution of data privacy laws across the globe.

The privacy laws have largely succeeded in defining what constitutes personal data and establishing the rights of its owners towards protecting their personal data. However, it should be borne in mind that such rights although originating from fundamental rights (e.g.

UN Human rights declaration of 1948 or human rights enshrined in constitutions of different countries), are not absolute in nature. These rights could be infringed by the governments for purposes like national security, defense, public interest etc. which is quite understandable and generally allowed for within Privacy Regulations. Let's try to understand what constitutes Personal data and then what rights a data subject has.

Let us also understand some privacy terminologies, listed below:

Data subject is the living individual whose data is processed.

Data controller is the organisation which has a purpose for using the data and establishes the means of processing personal data.

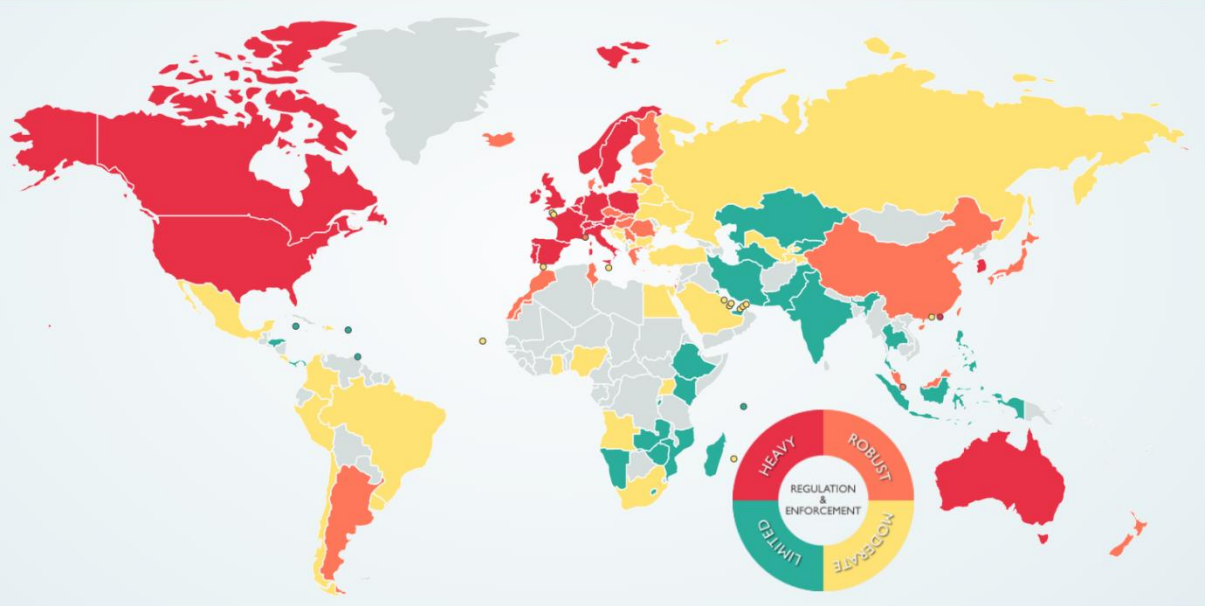
Data Processor is the organisation which processes the personal data on behalf of the data controller.

Most privacy laws require data controllers to collect **consent** of the data subject, implicit or explicit, before it can capture, store or process its personal data which is essentially an individual's permission to data controller for allowing it to process personal data. Any non-compliance of such a request is viewed very seriously by regulators as it is normally considered a breach of data subject's basic rights.

Notably, the controllers have some degree of liberty in processing personal data for an additional purpose if and only if such new purpose is commensurate with the original purpose for which the data was collected. Also, this holds true if personal data was collected for scientific research purposes, where the objective of such research could vary with its progression. Interestingly, the use of aggregated personal data of a large set of data subjects

without obtaining individuals' consents doesn't amount to denying data subject rights, till it is derived from data of large number of data subjects.

Data Protection Laws of the world



The above map depicts the rigor of data protection laws in different parts of the world. The 'Data Act' is the world's first national data protection law that was enacted in Sweden on 11 May 1973. EU GDPR is a privacy regulation is a culmination of several privacy frameworks, guidelines, directive and laws and is one of the most comprehensive data privacy regulations worth exploring. There are 12 Articles (Article 12 to Article 23) in EU GDPR that address data subject rights, however we shall examine the four most fundamental of these in details.

GDPR Article	Right of the Data Subject
Article 15	Right of access - Data subjects have the right to access data that a data controller has collected on them
Article 17	Right to erasure ('right to be forgotten') – Data subject may request for their personal data to be erased
Article 18	Right to restriction of processing - Data subjects can request that all processing of their personal data stop

Article 20	Right to data portability - Data subject can request controller to provide their data in a way that they can use it or send it to another controller without issues

Below are the data subject rights enshrined in the CCPA (California Consumer Protection Act) to be in force from 01 Jan 2020 which we have listed for comparison those in EU GDPR.

CCPA Section	**Right of the Consumer**
1798.100	Right to access and data portability – Consumers may request disclosure of personal information collected about them; if this information is provided electronically, it must be provided in a readily transferable electronic format
1798.105	Right to deletion – Consumers may request to have their person information deleted
1798.110	Right to request disclosure of information collected – Consumers may request an accounting of disclosures of personal information made to third parties
1798.115	Right to disclosure of information sold – Consumers may request an accounting of the disclosures, including sale, of personal information made to third parties
1798.120	Right to opt-out – Consumers may object to the sale of personal information about them

Comparison of Data Subject Rights between EU GDPR and CCPA.

1. **Right to Access:**

   GDPR Article 15 - The data subject get confirmation about whether personal data about him /her is being processed, but also access to certain information about that process.

   Exceptions: Aside from the uniform exception for manifestly unfounded or excessive requests, the right of access is only to be declined when the rights and freedoms of others are adversely affected.

CCPA Section 1798.100 - The Right to Access in the CCPA is not as extensive as the GDPR, but still requires that consumers have access to certain data collected by the business.

Exceptions: The CCPA does not provide for "exceptions" per se, but it is expected that the Attorney General may do so. Section 1798.185 specifically requires exceptions to be established for state or federal law compliance, such as trade secrets or other intellectual property.

2. **Right to Deletion**

Both the GDPR and the CCPA provide a right for deletion for data subjects. Although the two overlap in concept and ultimate execution, there are key differences in when and how an organisation must respond.

GDPR Article 17 - Right to Erasure ('right to be forgotten') - This right to erasure, despite the popular misconception, is not absolute (Article 17(3)). The controller may refuse to honour the request if continued processing is necessary.

3. **Right to Restriction of Processing**

This right is specific to GDPR but flows from denying a right to erasure. The CCPA does not have a similar provision.

CCPA - Like GDPR, the CCPA Section 1798.105 provides consumers the right of deletion - they may request that businesses delete their personal information.

GDPR Article 18 - This right provides that individuals may request that their data not be processed. Asserting this right can help those who would like their data erased, but the data cannot be erased.

Data subjects may request and obtain cessation of processing (Article 18(1)) when: Article 21 provides the legal bases of processing data, specifically legitimate interest and performance of a task in the public interest or authority vested in the controller.

Exceptions

The exceptions under this right are limited to the establishment, exercise, or defense of legal claims, to protect the rights of another natural or legal person, or for important public interests. Storage does not count as an exception, because 1) storage is the only processing that can be done if all others stop and 2) if storage was not allowed, it would be data erasure.

4. **Rights to Data Portability -** This right supports the free flow of information, provides user control and empowerment, and fosters competition and development of new services.

   GDPR Article 20 - Right to Data Portability - This right applies when the processing is based on consent, is done under contract in which the individual is a party (or is part of the steps taken to enter into a contract), or the processing is automated.

   Exceptions - Exceptions under this right are limited to processes in the public interest, exercise of official authority vested in the controller, and if it impacts the rights and freedoms of others.

   CCPA section 1798.100(d) - This right is included in the right to access and simply requires that if the data is "provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance." The GDPR is much more prescriptive.

   Clearly, data subject is the rightful owner of personal data and is either entitled to consent or withdraw consent for processing his personal data fully or partially, temporarily or permanently. It is only the government(s) that can take control of personal data without obtaining consent if it is required as per provisions of law, however there are still protections of various forms.

The examples of GDPR and CCPA are illustrative of the rights of the data subjects, however other national privacy laws may vary in their approaches of defining personal data and data subject rights. Privacy laws address the rights for children and vulnerable data subjects with higher rigor. Also, industry specific privacy standards like Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH) have special requirements in view of sensitive patient data that they specifically cover.

The privacy laws have empowered the regulators to impose large fines if data controllers and processors fail to protect the personal data or uphold the data subject rights. British Airways (BA) was fined a record £183 million [~$230 million], the highest data breach penalty to date and surpassing the $148 million Uber paid out in 2018. Cyber-criminals stole payment card details of an estimated 500,000 BA passengers that comprised the passenger's name, travel plans, billing address, email address and payment card details, and the three-digit security code. The UK's Information Commissioner Office had said its investigation found "poor security arrangements at the company" led to the breach. This shows that the regulation does have real teeth and the data protection authorities aren't afraid to exercises their powers.

With increasing use of technologies like Internet of Things (IoT), Wearable Technologies, Artificial Intelligence and Machine Learning, protecting data subject rights will continue to be a challenge for IT Audit and Security professionals. With enormous benefits for businesses using such technologies in the delivery of goods and services, there are also enormous threats posed to data protection. EU GDPR Art 22 comes to data subject's rescue and states that the data subject shall have the right not to be subject to a

decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

The privacy laws mark a shift in expectations of customers, and enterprises need to work harder to gain and maintain customer trust. Providing customers more control and choice over their data will give enterprises a competitive edge. More and more nations are fast embracing sound privacy laws so that they are not left out of trade relationships that seek protection of personal data. For example, India, the world's most populous democracy and an emerging market has recently tabled the Indian data protection bill in its parliament.

Despite some degree of variations in privacy laws and their enforcement across the world, today the data subject has clearly emerged as the owner of his/her own data and is empowered to decide whether, by whom or how it should be used. It is because, the world has recognized protection of personal data as a fundamental right of everyone.

References:

1. https://gdpr-info.eu/
2. https://enterprise.verizon.com/en-gb/resources/reports/dbir/2019 : 2019 Data Breach Investigations Report by Verizon
3. https://info.trustarc.com/managing-ccpa-gdpr-individual-rights-dsar-compliance.html
4. https://www.dlapiperdataprotection.com : (For publicly available graphics - no copyright)
5. https://researchdirect.westernsydney.edu.au/islandora/object/uws:52926/ Data privacy in Malaysia with the emergence of big data and artificial intelligence
6. https://medium.com/@dawn_91918/caring-about-the-corporate-invasion-into-your-personal-life-327633e9cf73 : (For publicly available graphics - no copyright)

About the Author: Sanjay, CISA, Fellow in Information Privacy(iapp.org) and PDP (bcs.org). He is a Cyber Security Consultant at Tata consultancy services, London. He is also Director at ISACA, London Chapter and has published Data Privacy article in ISACA London newsletter.