GA6: Legal

CIMUN

Topic 1: Eradicating the collection and sharing of personal data by private bodies

Krish Bhatia and Lucia Pitman

Introduction

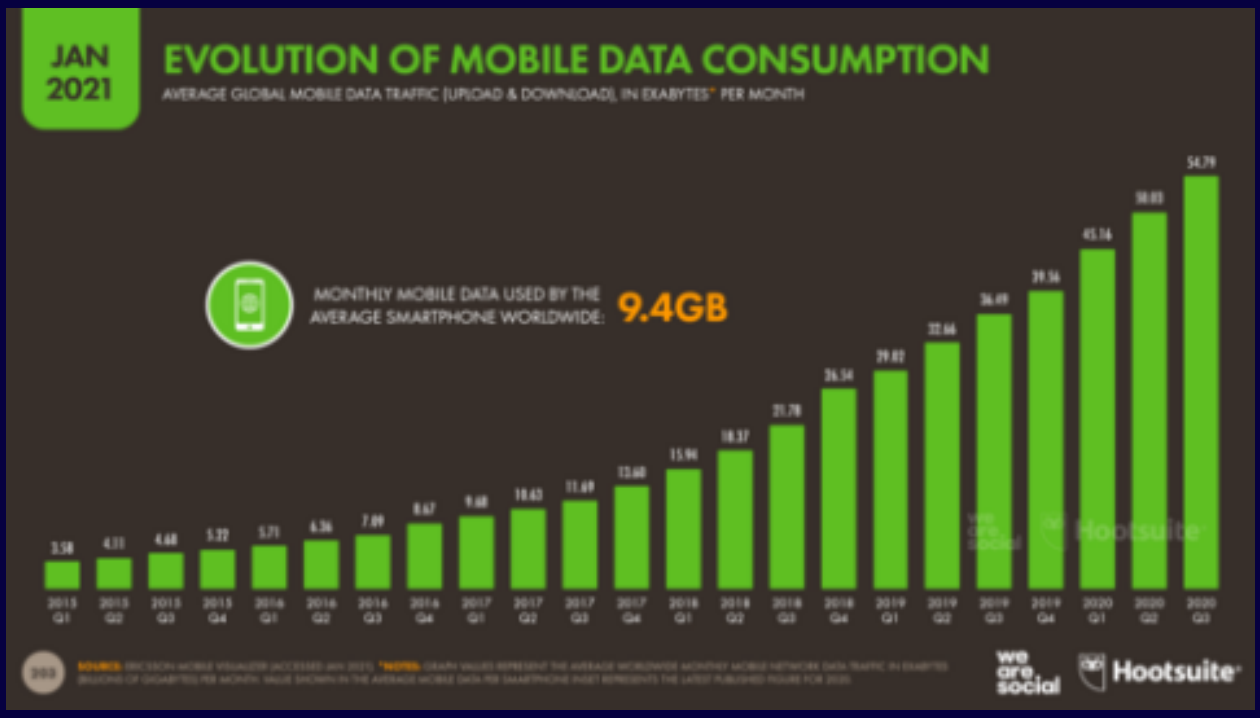
Why in a time where people are so willing to share the most private personal data online should there be so much regulation/discussion about protecting the privacy of personal data?
Most people don't realise that the most simple act of looking up something online will profile you together with thousands of other people. Private data covers such a wide range of sensitive things like one's religious beliefs, political views and opinions which are all personal and inherently innocent which can be taken by private bodies and shared and potentially misused. This data when added together is valuable and tradable information, but should not be so without the prior consent of an individual whose data has been taken. It is also regarded as an important aspect of human rights as it falls under the right to privacy.

Key terms

Eradicating - to get rid of something completely or destroy something bad (negative)
https://dictionary.cambridge.org/dictionary/english/eradicate
Collection - a group of objects of one type that have been collected by one person or in one place
https://dictionary.cambridge.org/dictionary/english/collection?q=collection+
Sharing → or more specifically data sharing - Data sharing usually means disclosing personal data to third parties outside your organisation. It can also cover the sharing of personal data between different parts of your own organisation, or other organisations within the same group or under the same parent company.
https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/9-data-sharing/#:~:text=What%20do%20you%20mean%20by,under%20the%20same%20parent%20company.
Personal data - Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.
https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en
Private bodies - private body means any legal entity established under private law which has a legal personality distinct from that of its founders/owners/members and which can exercise rights and be subject to obligations.
https://www.lawinsider.com/dictionary/private-body

Background

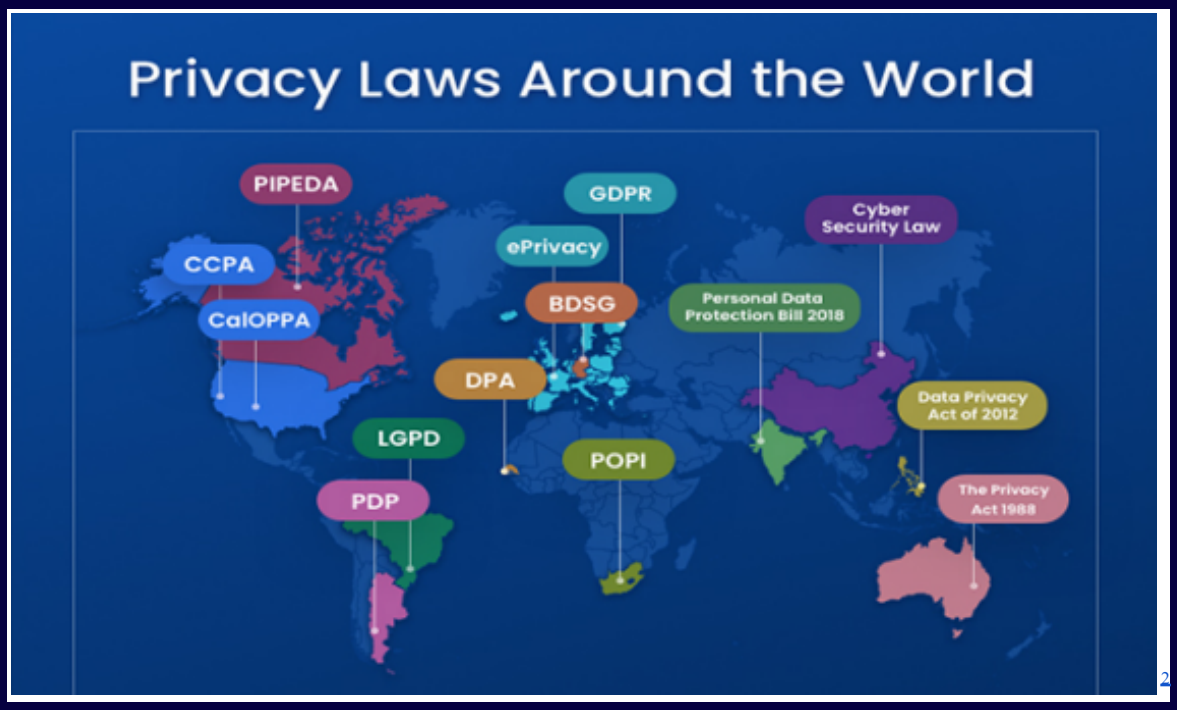
After the events of the first two world wars and the sheer amount of human rights that had been broken became clear, the Universal Declaration of Human Rights was created, published on December 10, 1948. It stated that ‘Everyone has the right to the protection of the data that concern them in order to ensure respect for their dignity, identity and privacy’. Although at that point there was not much open sharing of data. As the world has developed and the commercialisation of computers occurred, the data economy grew like never before. Companies finding great value in the collection and sharing of people's personal data. It became easier to collect personal data and share personal data. As personal data almost ceased to be personal, taking away the right to an individual to control what information about them became open to anyone. Privacy is the right of an individual to be free from uninvited surveillance. To safely exist in one’s space and freely express one’s opinions behind closed doors is critical to living in a democratic society. “Privacy forms the basis of our freedom. You have to have moments of reserve, reflection, intimacy, and solitude,” says Dr. Ann Cavoukian, former Information & Privacy Commissioner of Ontario, Canada. Dr. Cavoukian is best known for her leadership in the development of Privacy by Design (PbD), which now serves as a cornerstone for many pieces of contemporary data privacy legislation. But yet economical growth was linked to the sharing of data. Countries had to find a way for personal data to still be shared, but safely. Hence countries began to locally set personal data handling rules and laws. This unfortunately was still not good enough for international trade, as for sharing data across countries it was very difficult to adhere to greatly different legislations. The data privacy directive was the very first attempt of the European Union to set up ground rules for all of their member states in accordance with data privacy sharing. More legal enforcement where yet necessary because directives were not enforced by all countries, all having their own interpretations of the directive. Then the General Data Protection Regulation (GDPR) was imposed in 2016 with its effective date in May 2018, to get general coherence between countries. The European Union already has coherent laws, although they are still evolving. While countries outside the EU have started to also take the initiative to implement data privacy laws. Aside from the legislative part, what does GDPR and Data security do? It has a direct and significant impact on any private body which handles personal data. In short,anyone who is processing personal data has to follow the set regulation, and if not doing so effectively can be penalised or fined by the appointed authorities. Personal data includes a wide range of things from one's IP address to their religious beliefs. When processing personal data companies have to do it in adherence with the 7 principles (of GDPR); Lawfulness, fairness and transparency, Purpose limitation, Data minimization, Accuracy, Storage limitation, Integrity and confidentiality, Accountability. In practical terms they must have a lot of measures in place to have accountability and to take responsibility for lawful and safe data sharing, involving consent of the individual whose data is being shared.



[1]

This is a visual of the ever increasing use of mobile devices and online activity, to portray how much time people are spending on their devices, this getting profiled and sharing personal data (both willingly or unwillingly). As we delve deeper into this digital age, it can be seen that the amount of data in general online is increasing, meaning that it is becoming increasingly easier to find and take personal data from others.

[1] https://datareportal.com/reports/digital-2021-global-overview-report



[2]

Major countries and organisations involved

Even though Europe had a head start on the implementation of a legal framework, many other countries are taking into action other similar measures. Moreover, there can not be a law without enforcement, the enforcement bodies are data privacy authorities located in each country and organised so that if there's a dispute in Europe for example, there is a representative body to settle any conflict. Any citizen can report to the authorities if there is a data breach and the private sector goes under scrutiny. The countries that currently have data privacy laws (different variations per country listed) are; Argentina, Australia, Brazil, Canada, Chile, Colombia, Czech Republic, Denmark, Estonia, (European Union in general), Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, Ireland, India, Italy, Japan, Latvia, Lithuania, Luxembourg, Malaysia, Malta, Mexico, Morocco, The Netherlands, New Zealand, Norway, The Philippines, Romania, Poland, Portugal, Singapore, Slovenia, South Africa, South Korea, Spain, Switzerland, Sweden, Taiwan, United States, United Kingdom.

Relevant UN resolutions

The right to privacy is listed as a human right while other relevant resolutions include;

- The Right to Privacy in the Digital Age, 18 December 2013 (A/RES/68/167)
- The Right to Privacy in the Digital Age, 19 November 2014 (A/C.3/69/L.26/Rev.1)

[2] https://www.dreamcreationinfo.com/2019/07/privacy-laws-around-world-infographic.html

Previous attempts to resolve the issue

As previously stated, laws such as the GDPR regulation have been implemented in various countries. Laws that have been implemented throughout the years are;

In 1973, Sweden created the **first national privacy law called the Data Act**, which criminalized data theft and gave data subjects freedom to access their records.

In 1978, the German Federal Data Protection Act established basic data protection standards such as the requirement of consent for the processing of personal data. Consequently by 1979, many EU member states had incorporated data protection laws as fundamental rights into their legislation.

In 1983 – Right of Informational Self-Determination in Germany the German Federal Constitutional Court decided citizens should have a basic human right to self-determination over their personal data. In the ruling, it's established that individuals should be protected against the unlimited collection, storage, use, and disclosure of their personal data.

In 1995 – The EU Directive on Data Protection as computer technology advanced and free flow of information grew widespread, the European Union enacted the Directive on Data Protection, which imposed the minimum standards of personal data protection upon member states and protected the rights of individuals regarding the movement of personal data between EU member states. Under the directive, individuals had rights of access, access to supervisory authorities, and data was transferred outside of the EU so long as there was "an adequate level of protection". However, the law was implemented differently in each EU state, leading to some countries lacking stronger laws and oversight.

In 2000 – Safe Harbor Arrangement. This was a set of principles meant to rectify the different data privacy laws between the United States and the European Union to better facilitate the flow of information between the two regions. Ultimately, they were invalidated by the European Court of Justice in 2015 because under U.S. law, U.S. intelligence agencies had unrestricted access to the data of EU citizens. In 2016, the EU-US Privacy Shield was adopted to replace Safe Harbor, but its future was short as it was later also deemed inadequate.

In 2009 – Personal Data Privacy and Security Act of 2009. Over in the United States, data protection laws had been broken up by state. Beyond some legislation governing financial and health information, there was (and still is) no unifying federal legislation that protects the personal data of its citizenry at large. In 2009, a bill was proposed that would increase the protection of personal data by companies and government agencies, set restrictions on data sharing, and further criminalize identity theft and data privacy violations. The bill never passed.

In 2016 – The GDPR (General Data Protection Regulation). As data breaches and scandals soar, organizations around the world were given a two-year lead start to update security measures and protocols in time for the biggest set of data privacy laws yet. There are many provisions in the legislation, which seeks to unite the European Union under one set of stricter rules, including a right for data subjects to be forgotten, affirmative consent, comprehensive and timely data breach notifications, plain language for terms of service agreements, and fines of up to four percent of an organization's total worldwide annual turnover if found in violation.

Possible solutions

When looking into the possible solutions delegates should consider government control/entitlement to personal data, and the realistic implications of the complete eradication of the collection and sharing of personal data by private bodies on the economy. Transparency of the flow of data when talking about private bodies should also be looked at in relation to the more consenting side of the collecting and sharing of this data (If people don't know that their data/ how their data is being used, they will not have the power to control the flow of the data).

Bibliography

9. Data sharing. (2020, September 2). ICO. https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/9-data-sharing/

Collection defintion. (n.d.). Cambridge Dictionary | English Dictionary, Translations & Thesaurus. https://dictionary.cambridge.org/dictionary/english/collection?q=collection+

Data Privacy Laws around the world. (n.d.). Please Wait... | Cloudflare. https://www.privacypolicies.com/blog/privacy-law-by-country/

Declaration of Internet Rights. (n.d.). XVIII Legislatura -. https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_inglese.pdf

Digital 2021: Global overview report — DataReportal – Global digital insights. (2021, February 4). DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2021-global-overview-report

Eperi. (n.d.). Data Privacy Act: A brief history of modern data privacy laws. eperi Blog. https://blog.eperi.com/en/data-privacy-act-a-brief-history-of-modern-data-privacy-laws

Eradicate definition. (n.d.). Cambridge Dictionary | English Dictionary, Translations & Thesaurus. https://dictionary.cambridge.org/dictionary/english/eradicate

MUN report on - Legal measures to protect the use of personal data by social media companies. (n.d.). THIMUN Singapore – Welcome to THIMUN Singapore. https://singapore.thimun.org/wp-content/uploads/2019/09/GA6-1.pdf

Privacy laws around the world #infographic. (2019, July 25). Dream Creation: World,s Best Infographics Place. https://www.dreamcreationinfo.com/2019/07/privacy-laws-around-world-infographic.html

Private body definition. (n.d.). Law Insider. https://www.lawinsider.com/dictionary/private-body

What are the 7 principles of GDPR? (2021, April 12). ITEGRITI. https://itegriti.com/2020/compliance/what-are-seven-principles-gdpr/

What is personal data? (2019, 11). European Commission - European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en