UNIVERSITY of NICOSIA

Session 8

Privacy and Data Protection

BLOC 513: Law and Regulation in Blockchain

Session objectives

- Identifying key legislation regarding data protection and privacy in a variety of
- jurisdictions
- Identifying critical aspects of liability in data protection and privacy
- Understanding the interplay between blockchain immutability and the “right to be
- forgotten”

Session outline

1. Data protection & privacy in key jurisdictions.
2. Critical aspects of liability in data protection.
3. Blockchain immutability and the “right to be forgotten”.

Data protection & privacy in key jurisdictions

U.S Federally applicable Privacy Legislation

- The Health Insurance Portability and Accountability Act (HIPAA) has little to do with privacy and covers only communication between you and "covered entities," which include doctors, hospitals, pharmacies, insurers, and other similar businesses.
  - *People tend to think HIPAA covers all health data, but it doesn't.*
- The Fair Credit Reporting Act (FCRA) covers information in your credit report.
  - *It limits who is allowed to see a credit report, what the credit bureaus can collect, and how information is obtained.*
- The Family Educational Rights and Privacy Act (FERPA) details who can request student education records.
  - *This includes giving parents, eligible students, and other schools the right to inspect education records maintained by a school.*
- The Gramm-Leach-Bliley Act (GLBA) requires consumer financial products, such as loan services or investment-advice services, to explain how they share data, as well as the customer's right to opt out.
  - *The law doesn't restrict how companies use the data they collect, as long as they disclose such usage beforehand. It does at least attempt to put guardrails on the security of some personal data.*

NYT-The State of Consumer Data Privacy Laws in the US (And Why It Matters)

U.S Federally applicable Privacy Legislation

- The Electronic Communications Privacy Act (ECPA) restricts government wiretaps on telephone calls and other electronic signals (though the USA Patriot Act redefined much of this). It also sets broad rules concerning how employers can monitor employee communications.
- The Video Privacy Protection Act (VPPA) prevents the disclosure of VHS rental records.
  - *This law might sound silly now, but it came about after a journalist pulled the video-rental history of Supreme Court nominee Robert Bork.*
  - ***VPPA hasn't held against streaming companies, though.***
- The Children's Online Privacy Protection Rule (COPPA) imposes certain limits on a company's data collection for children under 13 years old.
- The Federal Trade Commission Act (FTC Act) empowers the FTC to go after an app or website that violates its own privacy policy.
  - *The FTC can also investigate violations of marketing language related to privacy, as it did when it issued a complaint against Zoom for deceiving users by saying video chats were end-to-end encrypted. Some groups have also recently called on the FTC to expand that power to abusive data practices.*

NYT-The State of Consumer Data Privacy Laws in the US (And Why It Matters)

California Privacy Legislation

- The California Consumer Privacy Act of 2018 (CCPA)
  - The CCPA applies to for-profit businesses that do business in California and meet any of the following:
    - Have a gross annual revenue of over $25 million;
    - Buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices; or
    - Derive 50% or more of their annual revenue from selling California residents' personal information
- Data broker:
  - They collect information about consumers from many sources including websites, other businesses, and public records. The data broker analyzes and packages the data for sale to other businesses.

- *The right to know about the personal information a business collects about them and how it is used and shared;*
- *The right to delete personal information collected from them (with some exceptions);*
- *The right to opt-out of the sale of their personal information; and*
- *The right to non-discrimination for exercising their CCPA rights.*
- *Businesses are required to give consumers certain notices explaining their privacy practices. The CCPA applies to many businesses, including data brokers.*

NYT-The State of Consumer Data Privacy Laws in the US (And Why It Matters)

E.U. General Data Protection Regulation

- The GDPR applies to:
  - a company or entity which processes personal data as part of the activities of one of its branches established in the EU, regardless of where the data is processed; or
  - a company established outside the EU and is offering goods/services (paid or for free) or is monitoring the behaviour of individuals in the EU.

- Circumstances when personal data may be processed:
  - with the consent of the individuals concerned;
  - where there is a contractual obligation (a contract between your company/organisation and a client);
  - to meet a legal obligation under EU or national legislation;
  - where processing is necessary for the performance of a task carried out in the public interest under EU or national legislation;
  - to protect the vital interests of an individual;
  - for an organisations legitimate interests

E.U. General Data Protection Regulation

- The GDPR provides the following rights for individuals:
  - The right to be informed
  - The right of access
  - The right to rectification
  - The right to erasure
  - The right to restrict processing
  - The right to data portability
  - The right to object
  - Rights in relation to automated decision making and profiling.
- Sensitive Data
  - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
  - trade-union membership;
  - genetic data, biometric data processed solely to identify a human being;
  - health-related data;
  - data concerning a person's sex life or sexual orientation.

Critical aspects of liability in data protection

Liability in Data Protection and Related Issues

- Data Transfers outside the E.U
  - A European Commission decision ('Adequacy Decision'), meaning that data can be transferred with another company in that third country without the data exporter being required to provide further safeguards or being subject to additional conditions. In other words, the transfers to an 'adequate' third country will be comparable to a transmission of data within the EU.

- Data Transfers outside the E.U
  - In the absence of an Adequacy Decision, a transfer can take place through the provision of appropriate safeguards and on condition that enforceable rights and effective legal remedies are available for individuals. Such appropriate safeguards include:
  - in the case of a group of undertakings, or groups of companies engaged in a joint economic activity, companies can transfer personal data based on so-called binding corporate rules;
  - contractual arrangements with the recipient of the personal data, using, for example, the standard contractual clauses approved by the European Commission

Liability in Data Protection and Related Issues

- Who is legally responsible for a breach?
  - In a cloud environment, under U.S. law (except HIPAA which places direct liability on a data holder), and standard contact terms, it is the data owner that faces liability for losses resulting from a data breach, even if the security failures are the fault of the data holder (cloud provider).

- Who is legally responsible for a breach?
  - Standard vendor agreement contracts exclude consequential damages and cap direct damages. In most cases, all damages flowing from a data breach of the data holder will be considered consequential damages and barred by a standard provision disclaiming all liability for consequential damages.
  - Agreements typically require by the data holder to report the data breach to the data owner and assist in the investigation.

Liability in Data Protection and Related Issues

- Identifying Liability
  - An entity failed to implement safeguards required by statute or reasonable security measures
  - An entity failed to remedy or mitigate the damage once the breach occurred
  - Failure to timely notify the affected individuals under a state's data breach notification statute, may give rise to liability for civil penalties imposed by a state attorney general or other state enforcement agency.

- Data breach response & mitigation
  - Nature of the infringement: - number of people affected, damaged they suffered, duration of infringement, and purpose of processing
  - Mitigation - actions taken to mitigate damage to data subjects
  - Past relevant infringements - has there been a pattern of negligence or incidents
  - Cooperation - how cooperative the firm has been with the supervisory authority to remedy the infringement
  - Certification: - whether the organization had qualified under approved certifications or adhered to approved codes of conduct

"Who is liable when a data breach occurs?"-Thompson Reuters

Blockchain immutability and the “right to be forgotten”.

Blockchain immutability and the “right to be forgotten”.

- Blockchain technology is one of the few that can guarantee almost total protection from accidental loss, destruction or damage and confidentiality
- It has also been proposed that blockchain and GDPR issues may be resolved by moving to a private, permissioned blockchain network that is designed in a way that each and every piece of data is readable by only the parties that absolutely need to, and can be rectified or erased at the request of the data subject
- By breaking the link between the wallet and the raw data since the private key is destroyed the raw data remains on the blockchain infrastructure, but it is no longer identifiable and therefore ought not to be considered as personal data under the definitions of the GDP

Required Reading

Required Reading

- Blockchain and the GDPR o EU Blockchain Observatory
  - https://www.eublockchainforum.eu/sites/default/files/reports/201 81016_report_gdpr.pdf

Further reading

Further reading

- Complete Guide to Privacy Laws in the US
  - https://www.varonis.com/blog/us-privacy-laws/

UNIVERSITY of NICOSIA

Questions?

Contact Us:

Twitter: **@mscdigital**
Course Support: **digitalcurrency@unic.ac.cy**
IT & Live Session Support: **dl.it@unic.ac.cy**