Module 2

The Five Cs of Ethical Data Science

Required

- Part II: Ethical Reasoning Beyond Privacy in Big Data from *Ethical Reasoning in Big Data: An Exploratory Analysis*
  - The Privacy Preferences of Americans
  - Engaging the Public in Ethical Reasoning About Big Data
  - Data Ethics—Attaining Personal Privacy on the Web

Recommended

- Hashim, M. J., Kannan, K. N., & Wegener, D. T. (2018). Central role of moral obligations in determining intentions to engage in digital piracy (Links to an external site.). *Journal of Management Information Systems, 35*(3), 934–963.
- Kho, N. D. (2019). AI, the IoT, and content: Ethics and opportunity (Links to an external site.). *EContent, 42*(3), 22–27.
- Wolkenstein, A., Jox, R. J., & Friedrich, O. (2018). Brain–Computer interfaces: Lessons to be learned from the ethics of algorithms (Links to an external site.). *Cambridge Quarterly of Healthcare Ethics: CQ., 27*(4), 635-646. http://dx.doi.org.csuglobal.idm.oclc.org/10.1017/S0963180118000130
- Microsoft General Technical Skills (2019). *Ethics and law in data analytics* (Links to an external site.) [Video]. LinkedInLearning.
  - Module 1: Data, Ethics, and Law

▼ What are data use agreements?

- These agreements are fruitful in establishing trust between data providers and data users.
- Data use agreements disclose what data is being collected.
- They also denote the reasons for using the data.
- Such agreements are often very restrictive, however, as they invariably take the form that the data provider either accepts or declines.
- Many agreements lack clarity and may not even have a legal basis. Such agreements are atypical of contractual negotiations in business where contracts are negotiated using multiple iterations.

▼ What is data sharing?

When a user is agreeing to a contract with a data service, the user either accepts the terms or the user does not get access. Such arrangements are usually non-negotiable.

▼ How may medical records may be used?

All patients at a medical facility must give consent to allow the facility to use their personal data. Typically, this data is saved, but there is no guarantee that the data is not used for other research purposes internal to the organization or facility.

▼ Data is a tangible asset. What does that mean for consent?

- In many cases, data is often sold without a user's consent.
- Moreover, there have been numerous data breaches that have occurred at organizations, such as Equifax, Experian, and Transunion. In these companies, consumers' personal data was compromised in a manner that could have a financial effect on the users.

▼ What is clarity?

- Users must be conscientious of the data they are providing to third parties.
- Users must be informed as to the processing that will be done with the data they provide.

- Users must be knowledgeable of the post-processing consequences of their data such as how it will be used to inform potential adverse actions against them.

▼ Why is consistency and trust crucial?

- Most data-collection entities exude good intentions when they collect data, but in most cases, they fail to honor those intentions when you need them to. Their illicit actions are generally granted great legal latitude.
- Once trust is broken with a data-collection entity, however, rebuilding the lost trust may generally take time.
- Consistent behavior, which demonstrates a commitment to being honest and sincere to the damaged parties, can enable the restoration of trust.
- Examples of such data-collection entities that have violated public trust include healthcare providers, government agencies, and data brokers.

▼ How much control does an individual have over the data they provide?

- When a data-collection entity such as Facebook asks for your views on politics or even gender, you cannot control what it decides to do with the data you provide. You have no recourse if you change your mind and want to rescind your data entries. If you decide to withdraw your data entries, you don't know whether Facebook actually deletes your information. In all likelihood, Facebook continues to use your information in ad placements.
- Users of internet apps have no control of their data usage due to minimal regulation. There are some limited choices available that make controlling access impossible. Europe's General Data Protection Regulation (GDPR) does have requirements that enable users to request their data to be removed and provided to them if requested.

▼ What is the Children's Online Privacy Protection Act (COPPA)?

The Children's Online Privacy Protection Act (COPPA) is utilized to provide protection for children and their data. This law is enforced by the Federal Trade Commission.

▼ What is the Genetic Information Nondiscrimination Act (GINA)?

The Genetic Information Nondiscrimination Act (GINA) was established to protect individuals from being discriminated against due to some adverse findings from genetic testing.