Case Studies Review:

Doing Data Science: A Framework and Case Study

and

Russia's War on Ukraine: Timeline of Cyber-Attacks

Ritesh Kumar

2024SP_MS_DSP_485-DL_SEC61: Data Governance, Ethics, and Law

Module 8

Second Case Studies Submission

Candice Bradley and Pushkar Shah

August 11, 2024

Table of Contents

Doing Data Science: A Framework and Case Study[1]

The Data

This case study on youth obesity in Fairfax County, Virginia, leverages a rich tapestry of data sources, including the American Community Survey, Fairfax County Youth Survey, property tax records, and geolocation data for food and recreational facilities. The authors meticulously detail these sources, delineating their geographic coverage and the data collection methodologies employed. However, the study confronted a formidable challenge: the absence of individual-level data, particularly vital health metrics like body mass index (BMI). This limitation constrained the researchers to descriptive statistics, curtailing their ability to conduct predictive analyses. The authors ultimately conclude that access to detailed, individual-level data is crucial for more robust and insightful analysis.

Relevance to Data Governance

This case study illuminates key facets of data governance, particularly in the context of data access, privacy, and the ethical use of sensitive information. The researchers encountered significant barriers in accessing individual-level data, likely due to stringent privacy regulations and ethical concerns surrounding minors' health data. This scenario underscores the intricate legal and ethical challenges inherent in data governance, where the imperative to protect personal privacy must be weighed against the potential benefits of public health research. The study underscores the delicate balance between safeguarding individual privacy and enabling thorough public health research, underscoring the need for more sophisticated data-sharing policies.

Relevant Legislation

[1] Keller et al., “Doing Data Science: A Framework and Case Study.”

While the study does not explicitly reference specific legislation, it operates within a legal framework shaped by key laws such as HIPAA[2], FERPA[3], and potentially COPPA[4]. Virginia's state-specific privacy laws and Institutional Review Board (IRB) regulations likely influenced the researchers' limited access to individual-level data. The authors advocate for alternative approaches to navigate data access challenges, calling for improved data-sharing policies that strike a balance between comprehensive analysis and privacy protection. They propose the development of new data governance frameworks, fostering trust through clear data-sharing protocols, and integrating ethical reviews throughout the research process. These recommendations highlight the need for more refined data governance legislation.

Data Governance Solution

The central takeaway is that, while essential for protecting privacy, current data governance practices can substantially impede critical public health research. The authors encountered significant obstacles in accessing the detailed, individual-level data necessary for a comprehensive analysis of youth obesity. Their recommendations for new data governance policies, enhanced data-sharing protocols, and ongoing ethical reviews may only partially address the complex challenges at the intersection of data privacy and research. Additional strategies, such as differential privacy, secure data enclaves, standardized anonymization protocols, tiered access systems, and public education on data privacy, could better balance privacy protection with research needs. This case study underscores the urgency of developing adaptable data governance frameworks that support data-driven research while maintaining rigorous privacy standards.

[2] "Health Insurance Portability and Accountability Act of 1996 (HIPAA)."

[3] "Family Educational Rights and Privacy Act (FERPA)."

[4] "Children's Online Privacy Protection Rule ('COPPA')."

Russia's War on Ukraine: Timeline of Cyber-Attacks[5]

The Data

The data in this case study comes from various sources, but the authors offer little detail on how it was collected and analyzed. Compiled by the European Parliamentary Research Service (EPRS), the briefing pulls from official EU documents, government reports, and credible media outlets like Microsoft, Politico, The Guardian, and Reuters. While these sources are cited, the methodology behind gathering and analyzing the data remains vague. Given the sensitive nature of cyber-attacks, some data likely comes from classified or protected sources. The timeline and examples provided offer a broad overview of the cyber dimensions of the Russia-Ukraine conflict, but a more thorough study would benefit from clearer explanations of data collection and analysis methods.

Relevance to Data Governance

This case study intersects with key aspects of data governance, highlighting management, legal, and ethical issues. From a management perspective, it stresses the need for robust cybersecurity measures to protect critical infrastructure. Legally, it raises concerns about sovereignty and international law, as these cyber-attacks often cross borders, challenging existing treaties. The EU's sanctions against perpetrators underscore the legal stakes. Ethically, the targeting of civilian infrastructure and the spread of disinformation raise serious moral questions, especially as independent hackers engage in counter-attacks, blurring the line between defense and vigilantism. The case underscores the complex interplay of these governance elements.

Relevant Legislation

[5] "Russia's War on Ukraine: Timeline of Cyber-Attacks."

The case study references key legislative and policy actions, including the EU's cyber-sanctions regime, first applied in July 2020 against those responsible for cyber-attacks, and the Strategic Compass initiative, which aims to bolster cyber-resilience through a new cyber-resilience act. It also mentions the EU's Permanent Structured Cooperation (PESCO)[6] framework, focused on cyber-defense projects, and several European Parliament resolutions calling for increased cybersecurity support to Ukraine. These actions point to existing legal frameworks but highlight the need for more targeted legislation to enhance international cooperation, clarify protocols for cyber-attacks, and protect critical infrastructure, particularly in global conflicts.

Data Governance Solution

The case study highlights the persistent cyber warfare between Russia and Ukraine, showcasing the evolving cyber threats in modern conflicts. While the authors don't offer a singular solution, they advocate for a multi-faceted strategy that includes international support, sanctions, strengthened capabilities, and improved legal frameworks. However, ongoing vulnerabilities suggest these measures might be insufficient. Additional solutions could include establishing a global cyber treaty, leveraging AI for cybersecurity, adopting zero-trust architectures, enhancing cyber education, and forming international rapid response teams. Improving attribution techniques and creating a global threat intelligence-sharing platform are also crucial. These approaches aim to address the global scale of cyber threats, promote proactive defense, and foster international collaboration, blending cutting-edge technology with human expertise.

[6] "Permanent Structured Cooperation (PESCO)."

References

[6] EEAS. "Permanent Structured Cooperation (PESCO)," n.d. https://www.eeas.europa.eu/eeas/permanent-structured-cooperation-pesco_en.

[4] Federal Trade Commission. "Children's Online Privacy Protection Rule ('COPPA')," February 3, 2023. https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa.

[1] Keller, Sallie Ann, Stephanie S. Shipp, Aaron D. Schroeder, and Gizem Korkmaz. "Doing Data Science: A Framework and Case Study." *Harvard Data Science Review* 2, no. 1 (January 31, 2020). https://doi.org/10.1162/99608f92.2d83f7f5.

[2] Public Health Law. "Health Insurance Portability and Accountability Act of 1996 (HIPAA)," July 10, 2024. https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge.

[5] Russia's war on Ukraine: Timeline of cyber-attacks. *EPRS | European Parliamentary Research Service*, June 2022. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf.

[3] US Department of Education (ED). "Family Educational Rights and Privacy Act (FERPA)," n.d. https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html#:~:text=FERPA%20gives%20parents%20certain%20rights,transferred%20are%20%22eligible%20students.%22.