Context Collapse Predicts Moral Injury from Cybersecurity Violations

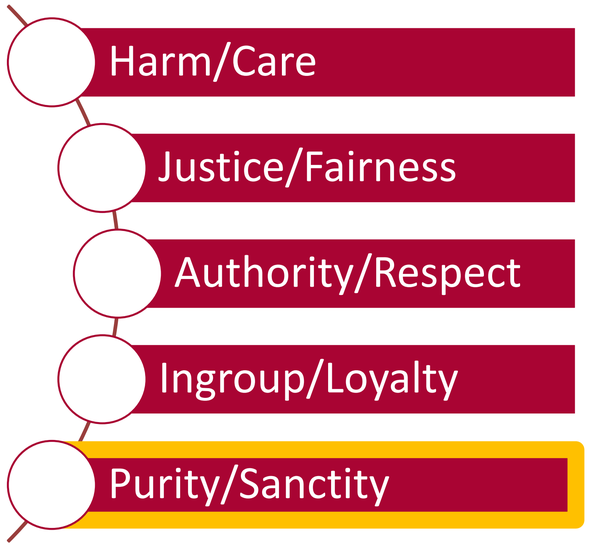
Noah Julius, Nathan Teh
Mentors: Ashlynn Main, Sherri Conklin

INTRODUCTION

- Cybersecurity is a field focused on data privacy and security, and ultimately, is about protecting people and preventing wrong from being done.
- Methods in fulfilling these goals is reflected in the five cybersecurity pillars, which can be divided into two groups: information security an information assurance.
- Current moral theory can aid in understanding what may further need to be done to ensure no wrong is done with respect to privacy and information flow.
- Using writings on contextual integrity and descriptions from Moral Foundations Theory (MFT) we can identify new wrongs that may not be accounted for in the cybersecurity pillars.
- This project looks at the 2015 Ashley Madison data breach to highlight privacy concerns highlighted by the above moral theories, bridging a gap between moral theory and concerns in cybersecurity.

METHODS

- **Literature Review** – Performed keyword searches looking for existing literature bridging cybersecurity and Moral Foundations Theory/ Contextual Integrity. No pieces were found making this specific bridge, giving us the gap to research.
- **Case Study Hunting** – To help form a bridge over this gap, we began searching for recent data breaches to highlight purity/sanctity violations from privacy breaches. In other words, a specific type of wrong. We selected the 2015 Ashley Madison data breach.
- **Case Study Analyses** – With our case selected, we began breaking down the case through the lens of MFT to understand what wrongs came from this breach.



MORAL THEORY

- **Moral Foundations Theory (MFT)**
  - A descriptive theory that states there are five core foundations that influence moral theory in cultures across the world
  - These foundations offer descriptions of the values that matter to us, giving insight on *what* was wronged in someone in events such as say data breaches.
  - This project focuses on the purity/sanctity foundation, the feeling of wrongness when something intended to stay inside, gets out and vice versa. We relate this to the feeling of violation when private data gets out into the public.
- **Contextual Integrity**
  - Integrity of data flow is dependent on its context, wrongs come from a collapse of this context when info flows between them in an improper manner.
  - The methods of obtaining information matter

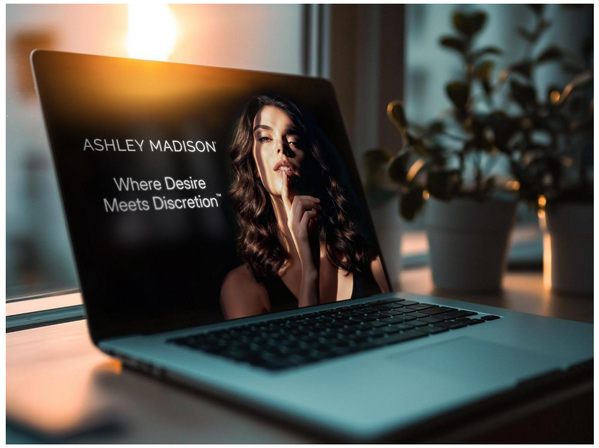


Photo from (Ashley Madison, n.d.) ashleymadison.com/en-us/

ASHLEY MADISON DATA BREACH

- Ashley Madison was a Canadian online dating service promoting extramarital affairs, with a slogan, “Life is short, have an affair”. Offering discreet dating.
- In July 2015 the hacker group called “The Impact Team” announced their access to Ashley Madison’s database with over 37 million users’ information. Which was then leaked after their demands to shut down the site were not met.

WHAT THIS HIGHLIGHTS

- Although it may have been appropriate for many of the users to have had their affairs brought to the public eye, there is still a wrong that comes from doing this via a data breach predicted by the violation of contextual integrity and realized as a moral injury to the purity/sanctity foundation.

WHAT’S NEXT

- Having selected a case study in the cybersecurity domain, we will analyze it through the lens of contextual integrity to evaluate whether the flow of information adheres to established privacy norms. Findings from this analysis will then inform a full research paper formalizing our framework and contributing to the broader literature on the application of privacy in cybersecurity.

REFERENCES

- Contextual Integrity: Nissenbaum, H. (2004), “Privacy as contextual20 integrity,” *Wash. Law Rev.,* vol. 79.
- Moral Foundations Theory. (n.d.). *Moral Foundations Theory*. https://moralfoundations.org/
- Huntress. (2025, November 11). *Ashley Madison data breach*. Huntress Threat Library. https://www.huntress.com/threat-library/data-breach/ashley-madison-data-breach

ACKNOWLEGEMENTS

This work is supported by funding for the VICEROY Northwest Institute for Cybersecurity Education and Research (CySER) provided by The Office of the Undersecretary of Defense for Research and Engineering, in collaboration with the Air Force Research Laboratory and Griffiss Institute.