

Thesis Portfolio

Mitigating Security Risks in Commonly Used Alexa Skills
(Technical Report)

**Balancing Care and Privacy: A Competition for Security Standards Governing Electronic
Medical Records**
(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Jammie Wang
Spring, 2021

Department of Computer Science

Table of Contents

Sociotechnical Synthesis

Mitigating Security Risks in Commonly Used Alexa Skills

Balancing Care and Privacy: A Competition for Security Standards Governing Electronic
Medical Records

Thesis Prospectus

Sociotechnical Synthesis

With the increased reliance on digital technology, some of the most important issues that experts are currently trying to address are privacy, security, and content moderation. Privacy and security are now more important than ever due to the digital presence that most people have developed. Moderating content and identifying where issues occur provides insight on how these privacy and security issues originate, and how they could potentially be fixed.

The need to address these issues led me to conduct research about frequently utilized digital technologies with privacy and security issues. The technical research report focuses on analyzing content moderation and security issues in Alexa skills. The STS research paper addresses the development of patient privacy laws governing electronic medical records.

The technical research report focuses on identifying common “risky” categories of Alexa skills, particularly those that exhibit privacy and security concerns. By parsing thousands of critical reviews across many categories of Alexa skills and searching for a set of “critical words,” the technical research aims to evaluate the frequency of these privacy concerns in comparison to the frequency of other types of concerns, namely financial concerns or concerns about inappropriate content. Most mentions of inappropriate content and financial complaints are from the “Games & Trivia” category of skills. Privacy and security concerns were present across all categories of Alexa skills, though less frequently than financial concerns. The “Kids” category appears to have a handful of skills that are particularly unsafe compared to the rest. Privacy concerns are more common in “Social”, “Kids”, and “Food & Drink” categories than financial issues. These results indicate that Alexa may need additional content moderation and stricter privacy policies to prevent skills from targeting vulnerable populations, such as children, for personal information.

As the number of daily cyberattacks on digital systems continue to grow, patient privacy is becoming a dominant issue within the healthcare community. The STS research paper examines the power dynamics between players who are responsible for creation of patient privacy laws. Patients are pushing for privacy law reform beyond HIPAA to better protect their medical data from unauthorized use or data leaks, yet corporations and hospitals will ultimately play a larger role in the formation of new laws due to their existing financial resources and the need to ensure future profit and research. As a “wicked problem,” there is no correct answer to how private data should be because it is a delicate balance between the common good and individual rights. However, literature review reveals that hospitals and insurance companies have spent vast amounts of money lobbying to prevent the implementation of new privacy practices. Since the use of electronic health records has been proven to be beneficial to the efficiency of hospital systems, Congress has allowed corporations and hospitals to continue the use of patient data despite patient calls for privacy reform.

Both research papers have demonstrated that privacy and security are key issues ranging across many aspects of daily life, from simply playing a game on an Alexa skill to getting medical treatment. Going forward, digital technology is only becoming more accessible and prominent. Thus, privacy and security are issues that should be addressed sooner rather than later, and new privacy laws should be expected within the near future.