

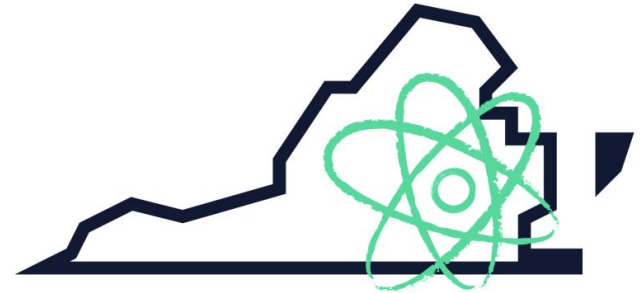


# COVES Fellowship with JCOTS

October 18, 2022



VIRGINIA ACADEMY OF  
SCIENCE, ENGINEERING AND MEDICINE



# COVES FELLOWS

COMMONWEALTH OF VIRGINIA  
ENGINEERING & SCIENCE FELLOWS



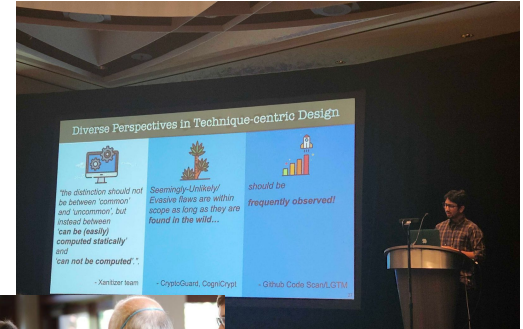
# AMIT SEAL AMI



*Ph.D. Candidate*

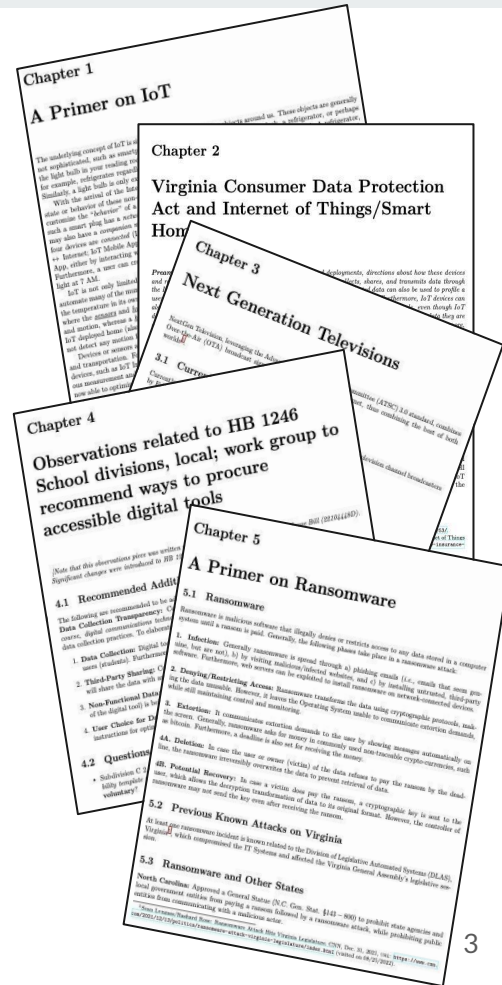
Cyber-Security and Software  
Engineering Researcher,

Systematic Analysis of Security  
Focused Techniques using  
Novel Research



# COVES Fellowship with JCOTS

- **Analyzed** Existing Policies, House Bills and Pertinent Issues
  - VCDPA, HB-1246, CCPA, GDPR, and more!
  - Ransomware; relevant Bills & Acts from Pennsylvania, NC, and the Federal Govt.
  - Next Generation Televisions
- **Created** Policy Briefs on IoT and Ransomware
- **Recommended** Steps for VCDPA in the context of IoT



---

# Virginia Consumer Data Protection Act (VCDPA) and IoT/Smart Homes - 1/2

VCDPA (§ 59.1-575 et seq.)

- Protects consumers' rights to data,
- Outlines the responsibilities and privacy protection standards for data controllers and processors, and
- Expected to be applied from 2023.



---

# Virginia Consumer Data Privacy Act (VCDPA) and IoT/Smart Homes - 2/2

## Smart Homes / IoT and Privacy Concerns

- Even simplistic IoT devices can profile users and record private behaviors
- Users expect to be informed of their rights related to data in a legally binding document
- In the context of existing Privacy policies, such as GDPR,
  - Significant gap between content and distribution of IoT device specific privacy policies,
  - Opportunities in terms of enforcement of data protection acts and compliance





# Recommended Step 1: Introduce Explicit Privacy Notice Distribution Guideline

## Context

VCDPA §59.1-578 C mentions that Controllers are expected to provide consumers with a reasonably accessible, clear, and meaningful privacy notice.

## Problem

- **43.52%** of vendors do not discuss smart home-related data or devices at all in their privacy notices
- **14.38%** IoT Vendors make IoT Device-specific privacy policies difficult to obtain

## Recommendation

Introduce explicit privacy distribution guidelines that specifies how device, website and service specific privacy notices are to be distributed to the consumers.



## Recommended Step 2: Enable Standards of Privacy Notices to facilitate Automated Analysis and Enforcement of Compliance

### Context

Controllers shall include

- i) The categories of personal data processed by the controller, and
- ii) the purpose for processing personal data

### Problem

- 69.01% privacy notices cannot be automatically analyzed due to unorthodox approach adoption
- 65.49% privacy notices do not specify data collection categories

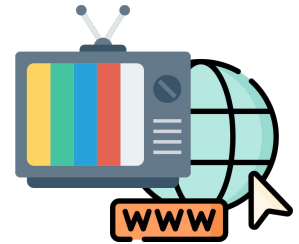
### Recommendation

Create/adopt a machine-readable standard for specifying and communicating privacy notices, that helps automate analysis and enforcement of privacy compliance.

# Next Generation Televisions

Combines the best of both worlds:

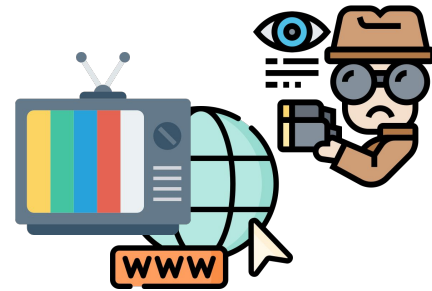
- Display broadcasted programs, with augmentations using the Internet
- Higher resolution (up to 4K Ultra High Definition Broadcast)
- Advanced Warning and Response Network System with remote triggers
- Bi-directional Communication between televisions and broadcasters





# Next Generation Televisions - Privacy Concerns

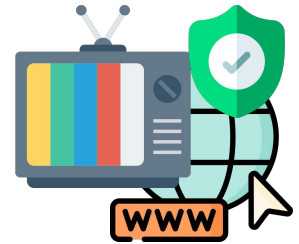
- Next-generation televisions establishes two-way connections between broadcasters and viewers, thus **enables viewer profiling**
- **Privacy violations are widespread** for *streaming service based channels*, such as Roku TV and Amazon Fire in the USA
- **Broadcasters focus on personalized advertisements** based on private data collected across social media accounts, location, and primary interests
- **Scope and type of data collection remains unclear** in the Next Gen TV standards, as of July 2022



---

## Next Gen Televisions - Recommendations

- CoV can introduce policies that can help protect public interest and privacy
- Roku TV limits privacy violation practices by default for all devices in European Union to comply with the General Data Protection Regulation (GDPR)



# Path Forward

We research on holistic cybersecurity

- Privacy Policies and their impact
- Evaluation of Security Compliance Enforcement Techniques
- Effectiveness of Compliance Enforcement



We also need to understand

- Diverse perspectives of policymakers,
- Trade-offs in policy making

**Let's continue the collaboration to continue making policies for greater public interest!**

Amit Seal Ami,  
aami at wm.edu, +1 757-839-4897  
<https://amitsealami.com/contact>

Research Labs:  
<https://spl-wm.github.io/>  
<https://www.cs.wm.edu/semeru/>