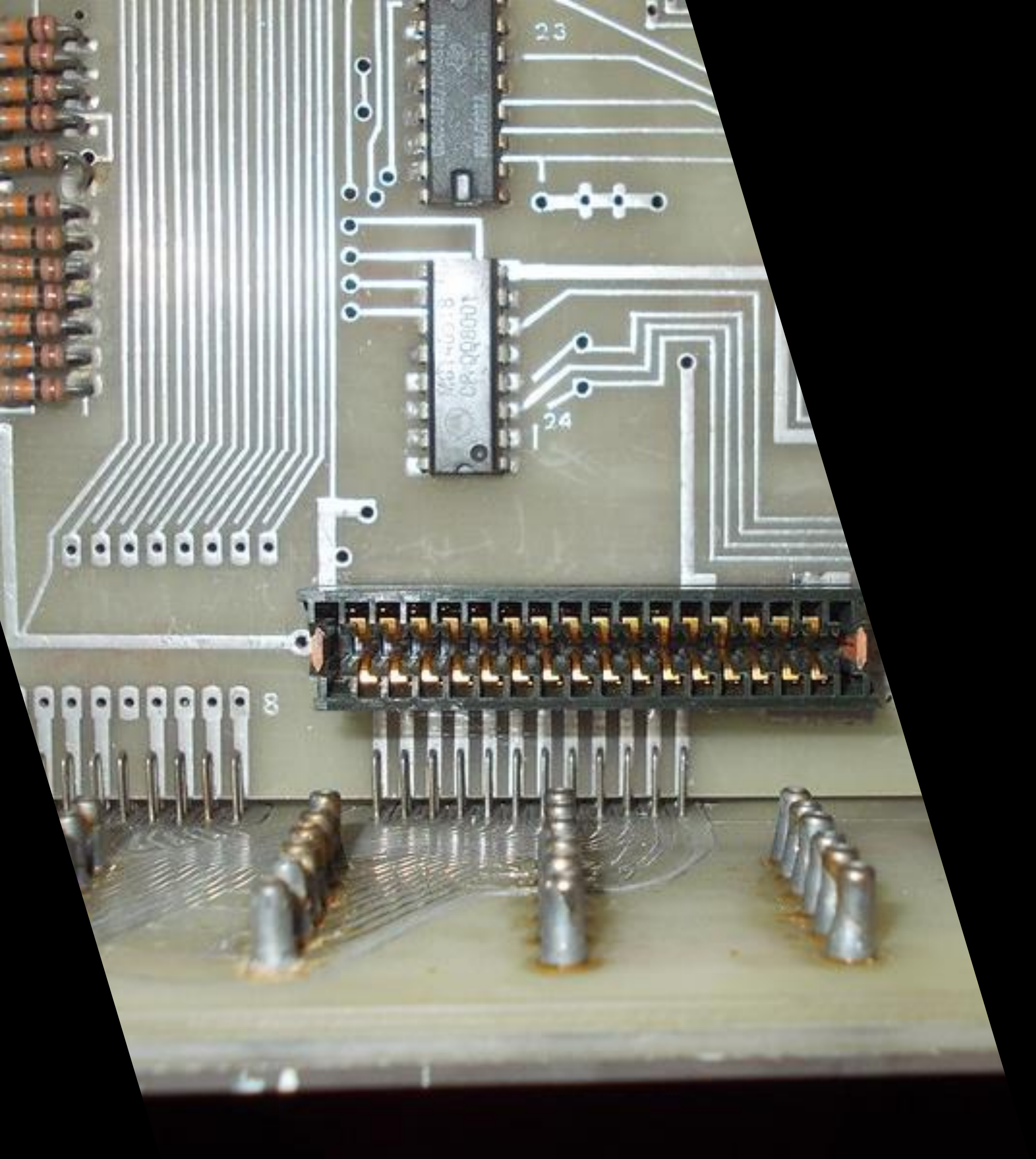
INVESTIGATING THE IOT- HARVESTING EVIDENCE WHILE MAINTAINING SUBJECTS' PRIVACY AND AUTONOMY

ABOUT ME

-Computer science student at MCC

-Cybersecurity student at UNO starting in January 2025

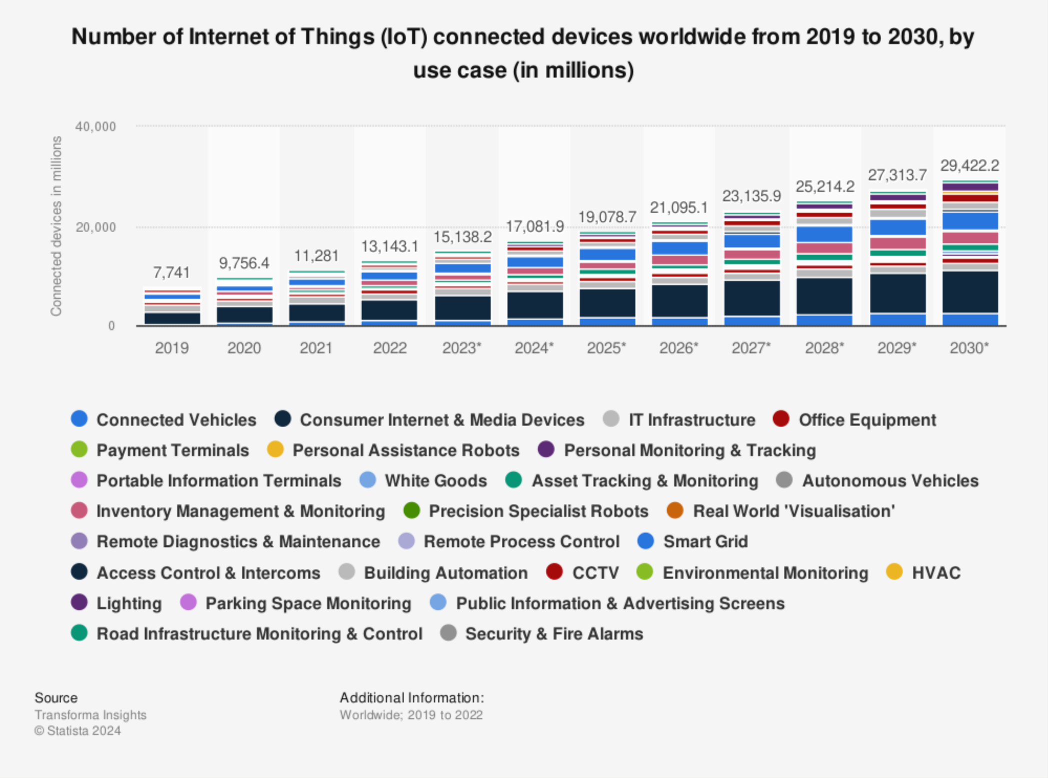
-Associates in video/audio arts from MCC, briefly worked in the field



OUTLINE

- Current digital forensics techniques for IoT devices
- Privacy and legal concerns for IoT forensic investigations
- Challenges and future research

THE RISE OF IOT



Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030, by use case (in millions)

Source
Transforma Insights
© Statista 2024

Additional Information:
Worldwide; 2019 to 2022

Chart source: *Statista*

- The popularity of Internet of Things (IoT) devices has skyrocketed in the past decade
- Benefits of network-connected devices:
  - Remote access
  - Easier updates and maintenance
  - Data collection for diagnostic troubleshooting
  - Data collection for analytics and marketing

Data collected by these devices can be useful in criminal and corporate misconduct investigations as evidence

DIGITAL FORENSICS TECHNIQUES FOR IOT

- IoT devices have minimal storage space/processing power
- Most investigation methods involve intercepting network activity
- Example: *IoTScent:*
    - Researchers connected Raspberry Pi to a network with smart home devices
    - Network traffic data was collected into CSV files
    - AI/ML can assist in parsing and interpreting data

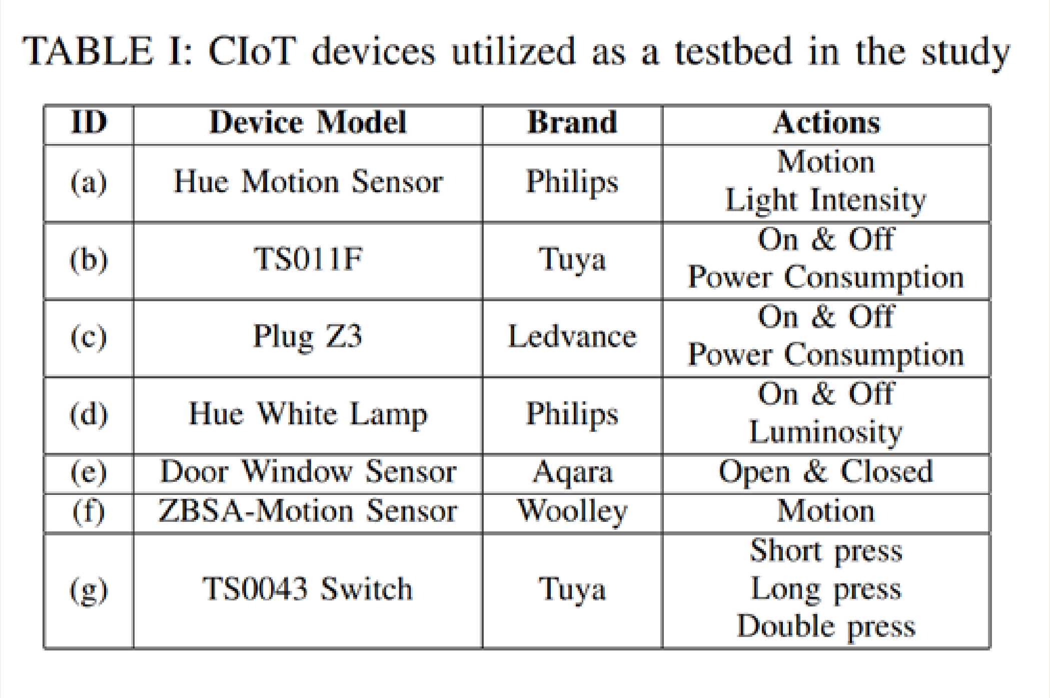


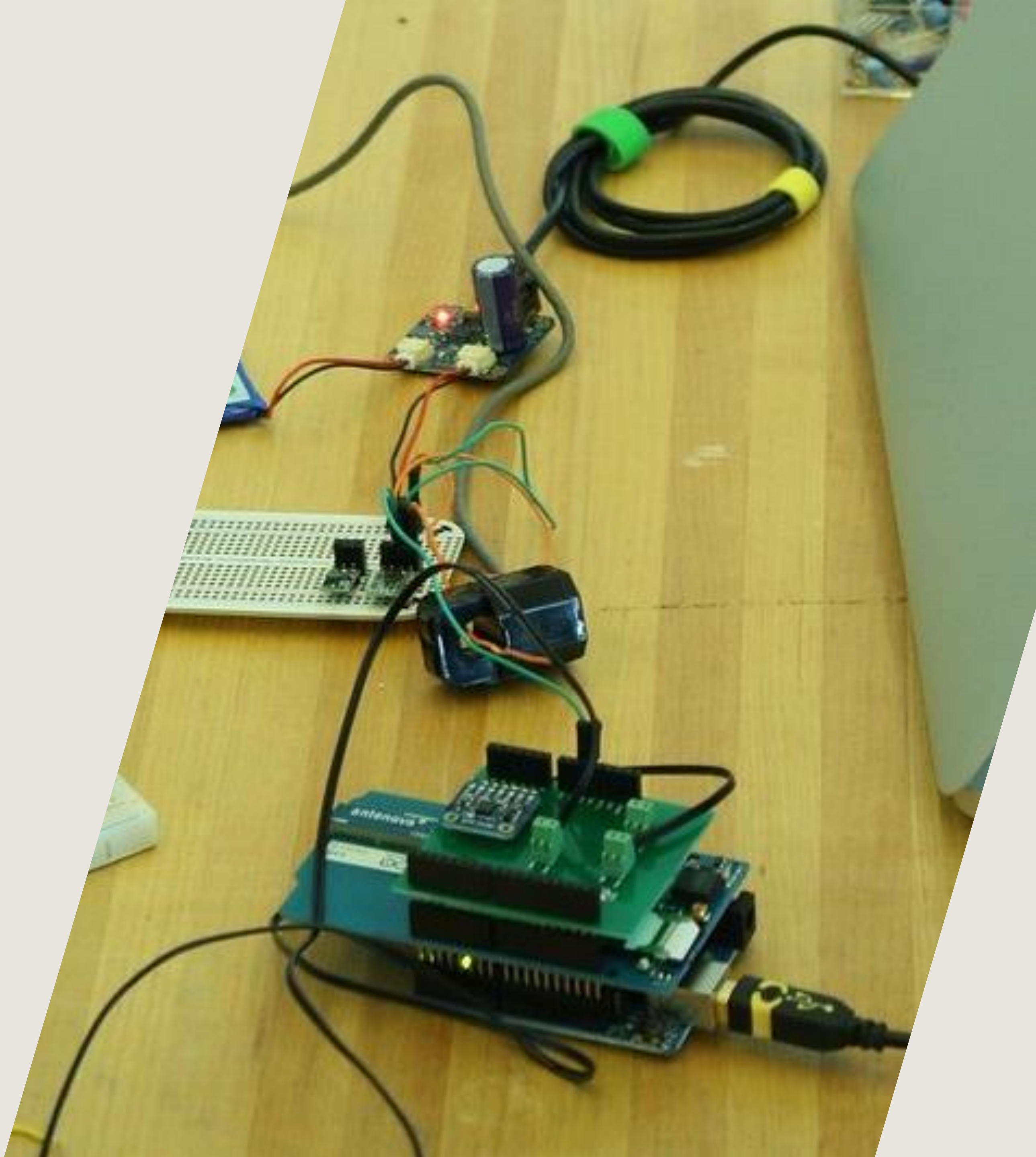
TABLE I: CIoT devices utilized as a testbed in the study

ID	Device Model	Brand	Actions
(a)	Hue Motion Sensor	Philips	Motion Light Intensity
(b)	TS011F	Tuya	On & Off Power Consumption
(c)	Plug Z3	Ledvance	On & Off Power Consumption
(d)	Hue White Lamp	Philips	On & Off Luminosity
(e)	Door Window Sensor	Aqara	Open & Closed
(f)	ZBSA-Motion Sensor	Woolley	Motion
(g)	TS0043 Switch	Tuya	Short press Long press Double press

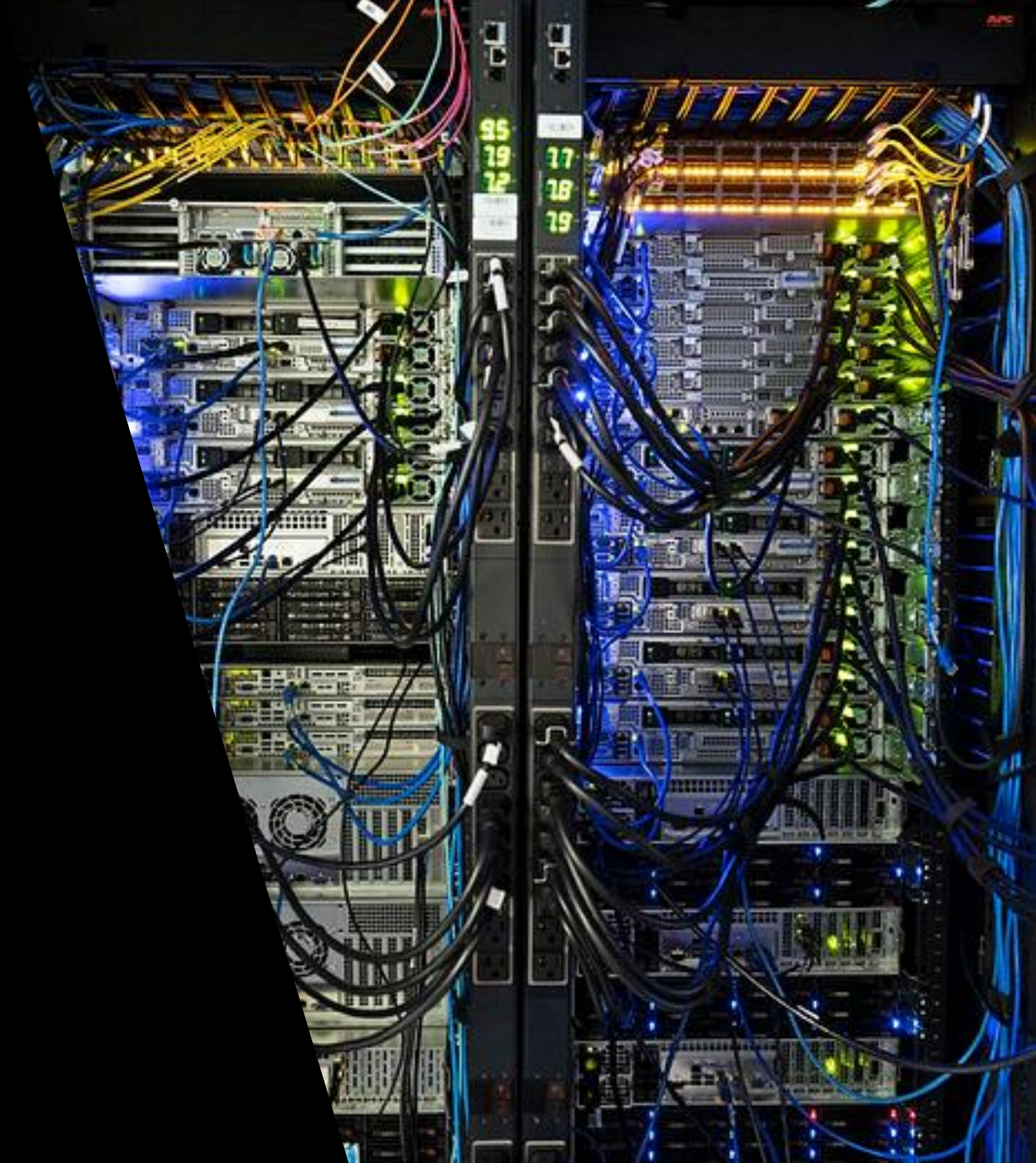
Image from: Boiano, A., Redondi, A., & Cesana, M. (2023). IOTSCENT: Enhancing Forensic Capabilities in Internet of Things Gateways. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2310.03401

TAKEAWAYS FROM *IOTSCENT*

- Tools can be developed that are compatible with multiple brands from different manufacturers
- IoT forensic investigation technology is still very limited



PRIVACY AND LEGAL CONCERNS



A DIGITAL PRIVACY FRAMEWORK

FROM: *A REFERENCE DESIGN MODEL TO MANAGE CONSENT IN DATA SUBJECTS-CENTERED INTERNET OF THINGS DEVICES*

1. **Explicit consent-** there should be no uncertainty on whether consent was obtained
2. **Transparency-** provide clear and comprehensive information on they are consenting to
   - Why their data is being collected
   - Examples of how the data is used
3. **Granularity-** allow multiple options or levels of consent instead of bundling all the terms and conditions together
4. **Age verification-** restrictions on data collections for minors
5. **Consent renewal and expiry-** include a clearly defined timeline where consent remains valid and when it must be renewed
6. **User interface-** a straightforward, intuitive way to interact with the device to complete the consent process without confusion

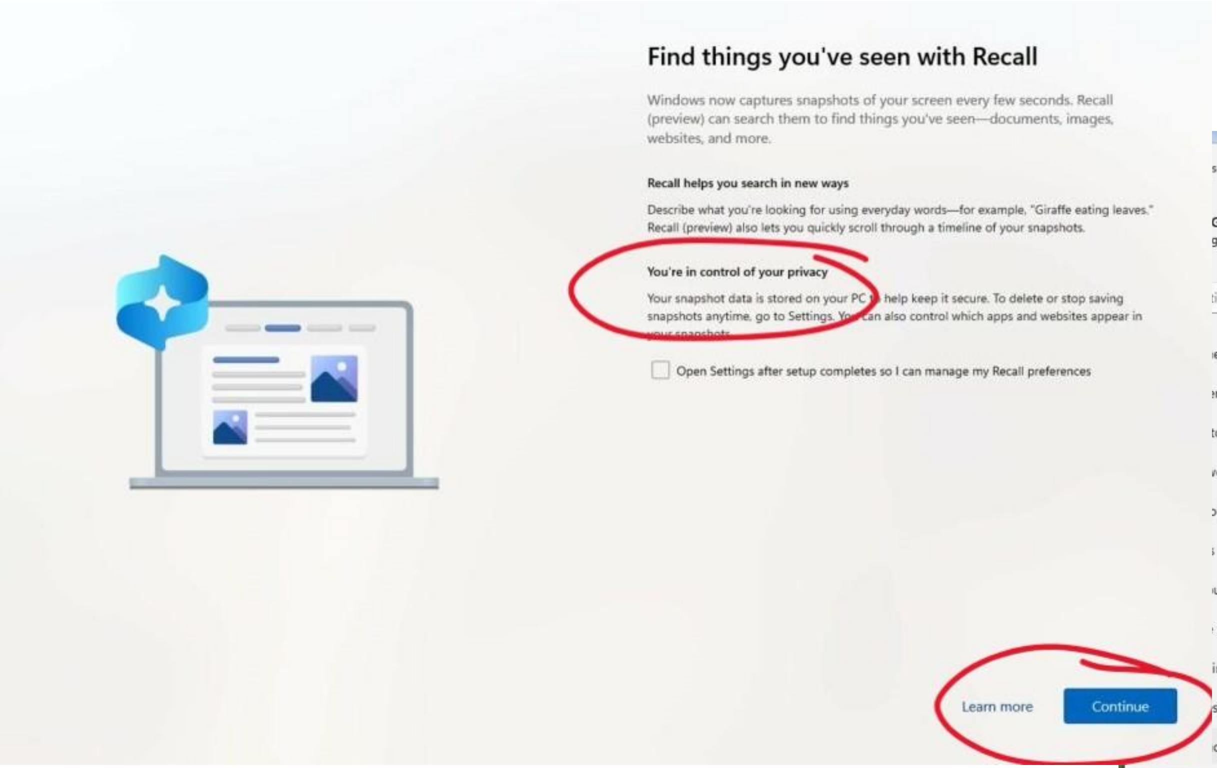
A DIGITAL PRIVACY FRAMEWORK, CONT.

7. **Withdrawal of consent-** users can easily withdraw consent at any time
8. **Communication-** users will receive consistent communication about updates or changes to data processing techniques
9. **Security and data protection-** all data is protected from unauthorized access or breaches
10. **Integration with systems-** consent management should be integrated with all systems that handle or process user data
11. **Auditing and compliance monitoring-** the consent management process should be constantly audited and monitored to catch issues with regulations and immediately remedy those issues

Legal experts should be consulted to tailor the consent process to specific products and cases

“WE CARE ABOUT YOUR PRIVACY!”

A BRIEF CASE STUDY- MICROSOFT RECALL



Find things you've seen with Recall

Windows now captures snapshots of your screen every few seconds. Recall (preview) can search them to find things you've seen—documents, images, websites, and more.

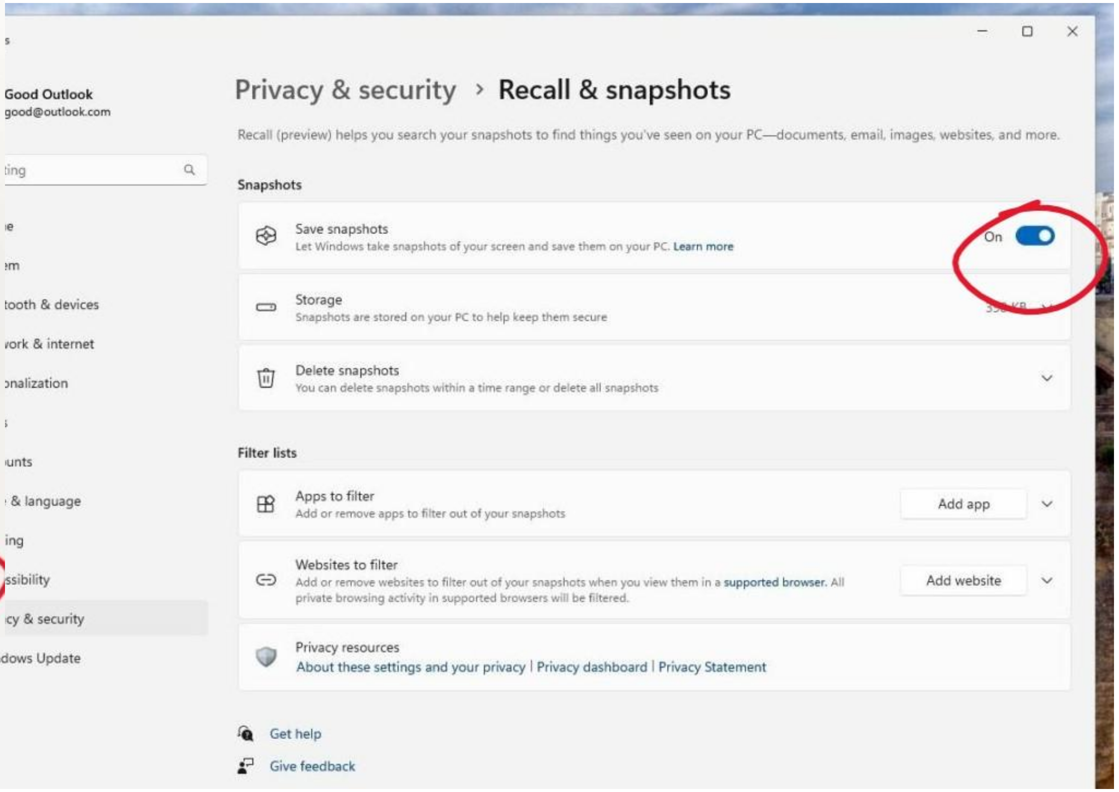
Recall helps you search in new ways

Describe what you're looking for using everyday words—for example, "Giraffe eating leaves." Recall (preview) also lets you quickly scroll through a timeline of your snapshots.

You're in control of your privacy

Your snapshot data is stored on your PC to help keep it secure. To delete or stop saving snapshots anytime, go to Settings. You can also control which apps and websites appear in your snapshots.

□ Open Settings after setup completes so I can manage my Recall preferences



Privacy & security › Recall & snapshots

Recall (preview) helps you search your snapshots to find things you've seen on your PC—documents, email, images, websites, and more.

Snapshots

Save snapshots
Let Windows take snapshots of your screen and save them on your PC. Learn more
On ●

Storage
Snapshots are stored on your PC to help keep them secure

Delete snapshots
You can delete snapshots within a time range or delete all snapshots

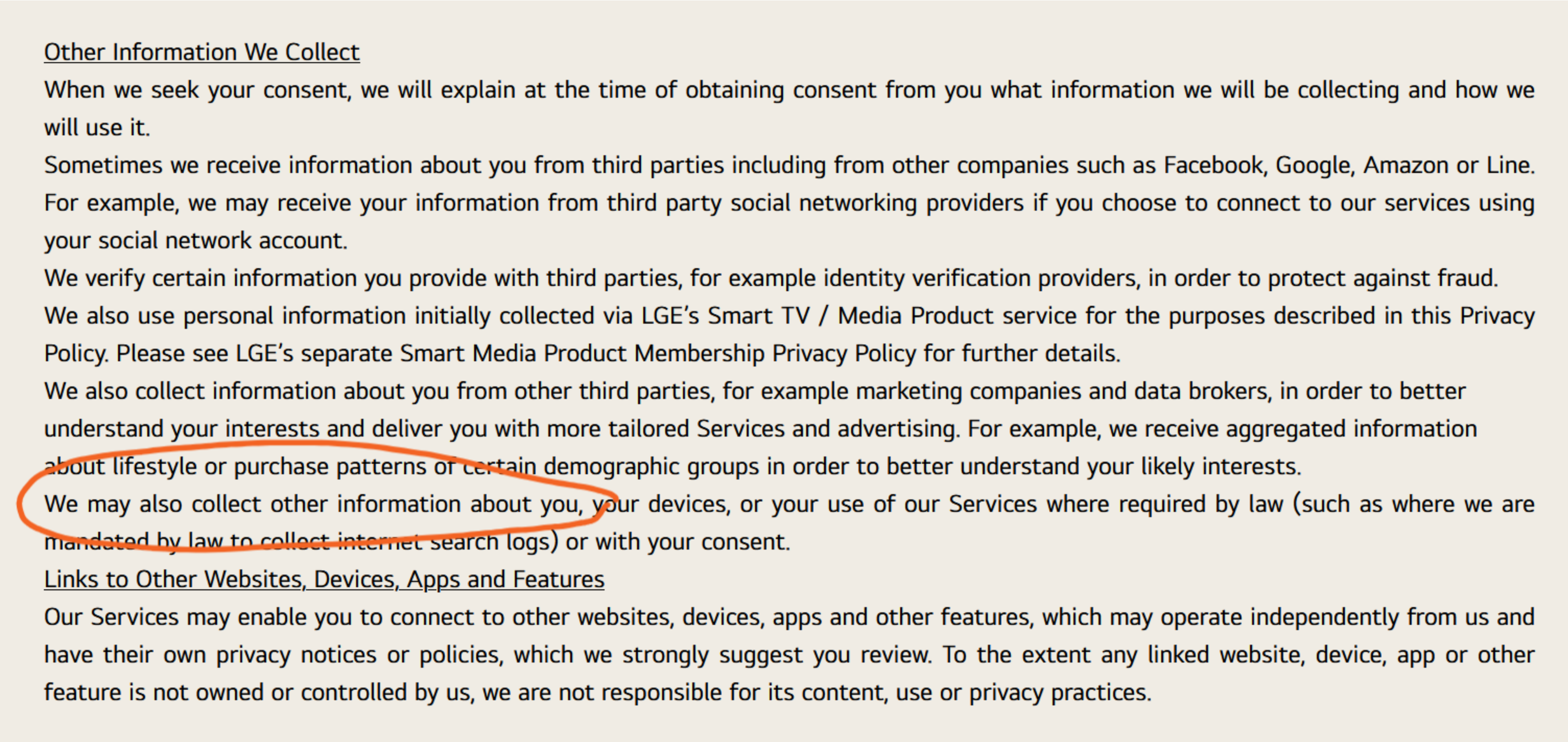
Filter lists

Apps to filter
Add or remove apps to filter out of your snapshots

Websites to filter
Add or remove websites to filter out of your snapshots when you view them in a supported browser. All private browsing activity in supported browsers will be filtered.

Privacy resources
About these settings and your privacy | Privacy dashboard | Privacy Statement

“WE CARE ABOUT YOUR PRIVACY!” A BRIEF CASE STUDY- LG GLOBAL’S SMART DEVICE PRIVACY POLICY



Other Information We Collect

When we seek your consent, we will explain at the time of obtaining consent from you what information we will be collecting and how we will use it.

Sometimes we receive information about you from third parties including from other companies such as Facebook, Google, Amazon or Line. For example, we may receive your information from third party social networking providers if you choose to connect to our services using your social network account.

We verify certain information you provide with third parties, for example identity verification providers, in order to protect against fraud.

We also use personal information initially collected via LGE’s Smart TV / Media Product service for the purposes described in this Privacy Policy. Please see LGE’s separate Smart Media Product Membership Privacy Policy for further details.

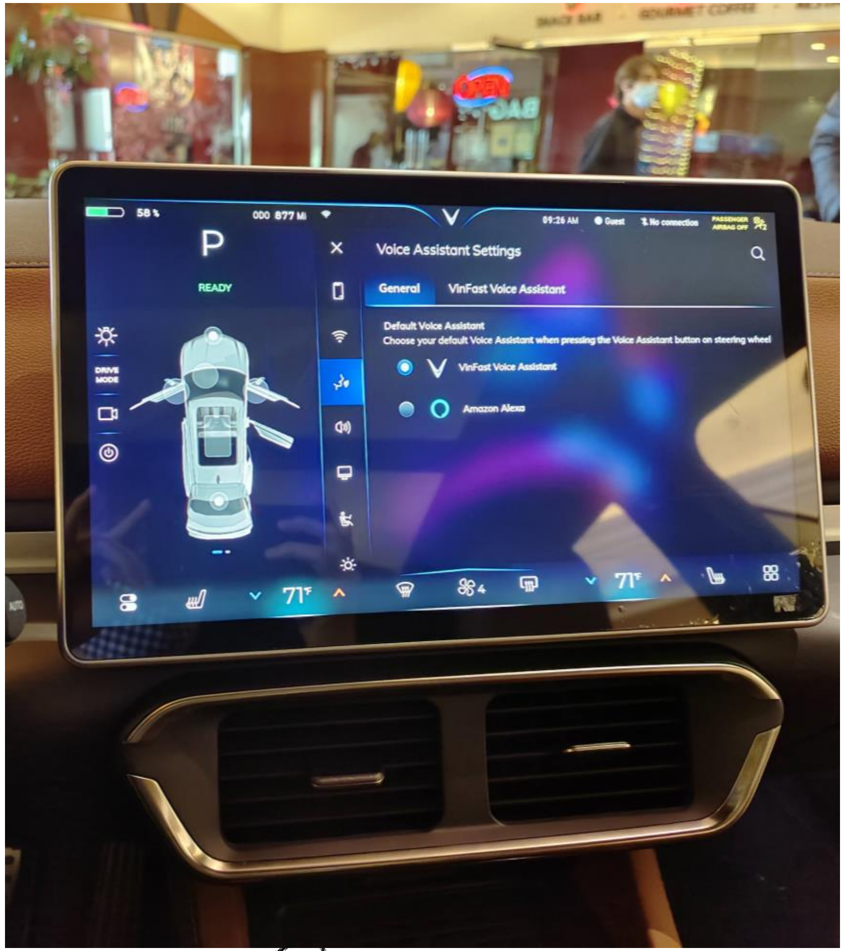
We also collect information about you from other third parties, for example marketing companies and data brokers, in order to better understand your interests and deliver you with more tailored Services and advertising. For example, we receive aggregated information about lifestyle or purchase patterns of certain demographic groups in order to better understand your likely interests.

We may also collect other information about you, your devices, or your use of our Services where required by law (such as where we are mandated by law to collect internet search logs) or with your consent.

Links to Other Websites, Devices, Apps and Features

Our Services may enable you to connect to other websites, devices, apps and other features, which may operate independently from us and have their own privacy notices or policies, which we strongly suggest you review. To the extent any linked website, device, app or other feature is not owned or controlled by us, we are not responsible for its content, use or privacy practices.

“WE CARE ABOUT YOUR PRIVACY!”
A BRIEF CASE STUDY- SUBARU PRIVACY POLICY



“Subaru’s privacy policy says that even passengers of a car that uses connected services have ‘consented’ to allow them to use -- and maybe even sell -- their personal information just by being inside.” (Mozilla Foundation, 2023).

Reference : *It’s Official: Cars Are Terrible at Privacy and Security*. (2023, September 6). Mozilla Foundation. https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/

IOT FORENSICS AND THE LAW

Writing and executing a search warrant for an IoT presents multiple difficulties:

- How to draft the warrant to match the scope of the investigation
- How to extract data from the device that is only relevant to the case and doesn’t breach the privacy of those not involved

The Electronic Communication Privacy Act of 1986 (ECPA) has general guidelines for digital privacy but is far too outdated to be applied to the IoT. What is considered an “electronic communication” protected by this law?

- A user activating a smart home assistant to turn off the light?
- Someone waving their hand by a smart faucet to turn it on?

Both could be used as key evidence in a court case

CHALLENGES AND AREAS FOR FUTURE RESEARCH

CHALLENGES: THE DATA DEFICIT

Bad actors are increasingly aware of their digital footprint, leading to newer anti-digital forensics techniques

- Limited investigation methods for IoT devices makes anti-forensics easier

Massive amounts of data is produced by the IoT, increasing the load of data for investigators to parse

- AI/ML could be helpful

Harvesting network activity instead of data from storage media is more challenging

CHALLENGES: NEW TRENDS IN TECH

- **Previously, computers were manufactured by only a few companies**
- **Certifications dedicated to specific tech brands**
- **More companies with proprietary software and hardware**

ACCESSDATA CERTIFIED EXAMINER
ACE
CERTIFIED FORENSIC MAC EXAMINER
CFME
GIAC ADVANCED SMARTPHONE FORENSICS
GASF
CERTIFIED ADVANCED WINDOWS FORENSIC EXAMINER
IACIS

Above: current digital forensics certifications

WHERE WE'RE HEADED

- ✓ Certified Smart Home Device Forensic Specialist
- ✓ Connected Critical Infrastructure Forensic Examiner
- ✓ Advanced Wearable Computer Device Forensic Specialist

AREAS FOR RESEARCH

- Developing tools to aid in IoT forensic investigations
- Advancing our understanding of human-device interaction patterns, distinguishing identities of people interacting with the device in the data collected
- Researching how to integrate IoT devices into the legal process, updating current legislation and introducing laws to add consumer protections, regulate data collection, and dictate how evidence from the IoT can be used in court

CONCLUSION

- Methods to perform forensics on IoT devices are currently very limited
- Using data from these devices presents numerous privacy and legal issues
- Further research is urgently needed to catch up with this new technology and laws must be updated

THANK YOU

Grace Swerczek

graceswerczek@gmail.com

LinkedIn: grace-swerczek