

4-5-2022

Digital Privacy in the Home

Kelley Flannery Rowan
Florida International University, krowan@fiu.edu

Follow this and additional works at: <https://digitalcommons.fiu.edu/glworks>



Part of the [Science and Technology Studies Commons](#)

Recommended Citation

Rowan, Kelley Flannery, "Digital Privacy in the Home" (2022). *Works of the FIU Libraries*. 109.
<https://digitalcommons.fiu.edu/glworks/109>

This work is brought to you for free and open access by the FIU Libraries at FIU Digital Commons. It has been accepted for inclusion in Works of the FIU Libraries by an authorized administrator of FIU Digital Commons. For more information, please contact dcc@fiu.edu.

Digital Privacy in the Home

from passwords
to the
internet of things

A Digital Scholar Studio workshop
Kelley Rowan, Digital Archives Librarian



Agenda

- PII v. personal information
- Threat assessment
- Risky behaviors
- Device security
- Passwords
- Privacy browsers
- VPN
- Healthcare



Internet of Things

- The home network
- Wearables
- Fertility apps
- The home network
- Smart TVs
- Smart assistants
- Nest & ring
- Cars
- Appliances



Personally
identifiable
information (PII)
&
personal
information

**What's the
difference?**

Personal (sensitive) =
information that identifies
you: social security number,
passport, drivers license/ID

PII = information that could
help identify you: the city
you live in, date of birth,
email

Threat Assessment

- What do you need to protect?
- Who do you need to protect it from?
- What are the consequences of a breach?
- Identify risky behaviors
- Identify your data risks
- Identify risky settings (devices & apps)



Risky behaviors

Computer,
phone, ipad lacks security

Browser stores your
passwords

Reusing the same
password or using weak
passwords

Revealing personal
information on social
media

Leaving digital items
accessible

Leaving bluetooth on
everywhere you go

Using public wifi for
sensitive tasks

Safe behaviors



Run updates

Turn off location

Keep your bluetooth off

Use biometrics

Minimize apps/data being stored and used

Only download trusted apps from sites such as Google Play or the Apple store

Extra security for android users - use VPN

Enable the "find my device" feature

Block most notifications and permissions

Device security

Facial
recognition

Password

Fingerprint

Pin number

Pattern

Voice
recognition

Strongest security options



BIOMETRICS



PASSWORD



+ 2FA

SMS 2FA

- SMS and MMS are being replaced by RCS (rich communication service)
- Confirm encryption



Creating a strong password



stL_+1?stLWrAziPl3we

✔ Strong password

- 12+ letters, symbols, and numbers
- Random capitalization
- Random pass phrases

A passwordless future?

The passkey is a FIDO (fast identity online) credential such as a fingerprint ID

Based on FIDO standards, passkeys are a replacement for passwords that provide faster, easier, and more secure sign-ins to websites and apps across a user's devices. Unlike passwords, passkeys are always strong and phishing-resistant.

<https://fidoalliance.org/passkeys/#~:text=Any%20passwordless%20FIDO%20credential%20is%20there%20are%20no%20shared%20secrets.>



Password & passphrase generators

- Norton password generator
 - <https://my.norton.com/extspa/passwordmanager?path=pwd-gen>
- Strong password generator.com
 - <https://privacycanada.net/strong-password-generator/>
- Strong password generator.org
 - <https://www.strongpasswordgenerator.org/>
- MSD Services
 - <https://www.msdservices.com/apg/>
- Diceware – will give you random words for passphrases
 - <https://diceware.dmath.org/>



This Photo by Unknown author is licensed under [CC BY-NC-ND](#).

Is it safe to let my browser store my passwords?

- Opinions range on this from low to average safety and security to not secure enough, use a password manager



This Photo by Unknown author is licensed under [CC BY-SA](#).

Norton password generator

WatRa3Wa+9L5*+!r1fAf



Copy Password

✓ Strong password

Use the slider, and select from the options, below, to lengthen your password and strengthen your security.

Password Length (4-64)

20

☒ Letters ☒ Mixed case ☒ Punctuation ☒ Numbers

Password managers

- Use AES 256-bit encryption
- Zero knowledge architecture
- 2FA recommended
- Generate strong passwords
- Scan the web for security breaches
- Include biometrics
- Update reminders
- *Avoid free managers
- *desktop is slightly more secure than cloud

Password Managers

- **Roboform (cloud) \$1.39/month**
 - <https://www.roboform.com/lp?frm=offer-digital-com&affid=digpw>
- **Dashlane (desktop) \$60.00/year**
 - https://www.dashlane.com/lp/summer21?utm_source=adwords&utm_campaign=US_Search_Brand_Exact&utm_medium=15594053097&utm_term=Dashlane&gclid=CjwKCAjw7--KBhAMEiwAxfpkWEmq6h9ovBxcByAVrq9ffRruOQhFdRkQ2BrckK05TfVgGbNGfkMwNJxoCZk4QAvD_BwE
- **NordPass (cloud and/or desktop) \$35.00-\$60.00/year**
 - https://nordpass.com/cybernews/?coupon=cybernews&utm_medium=affiliate&utm_term&utm_content=c36b351f-8f61-4c3a-9051-6c645efaa7b4&utm_campaign=off519&utm_source=aff41342&aff_free
- **LastPass (cloud) \$60.00/year**
 - https://www.lastpass.com/get-premium?utm_medium=cpc&gclid=CjwKCAjw7--KBhAMEiwAxfpkWC2zjtbkskFuyUAnjQj7RWZUmq11hzS6v69QpvMDcHC4HYnat_UOVBoCkYIQAvD_BwE&gclsrc=aw.ds

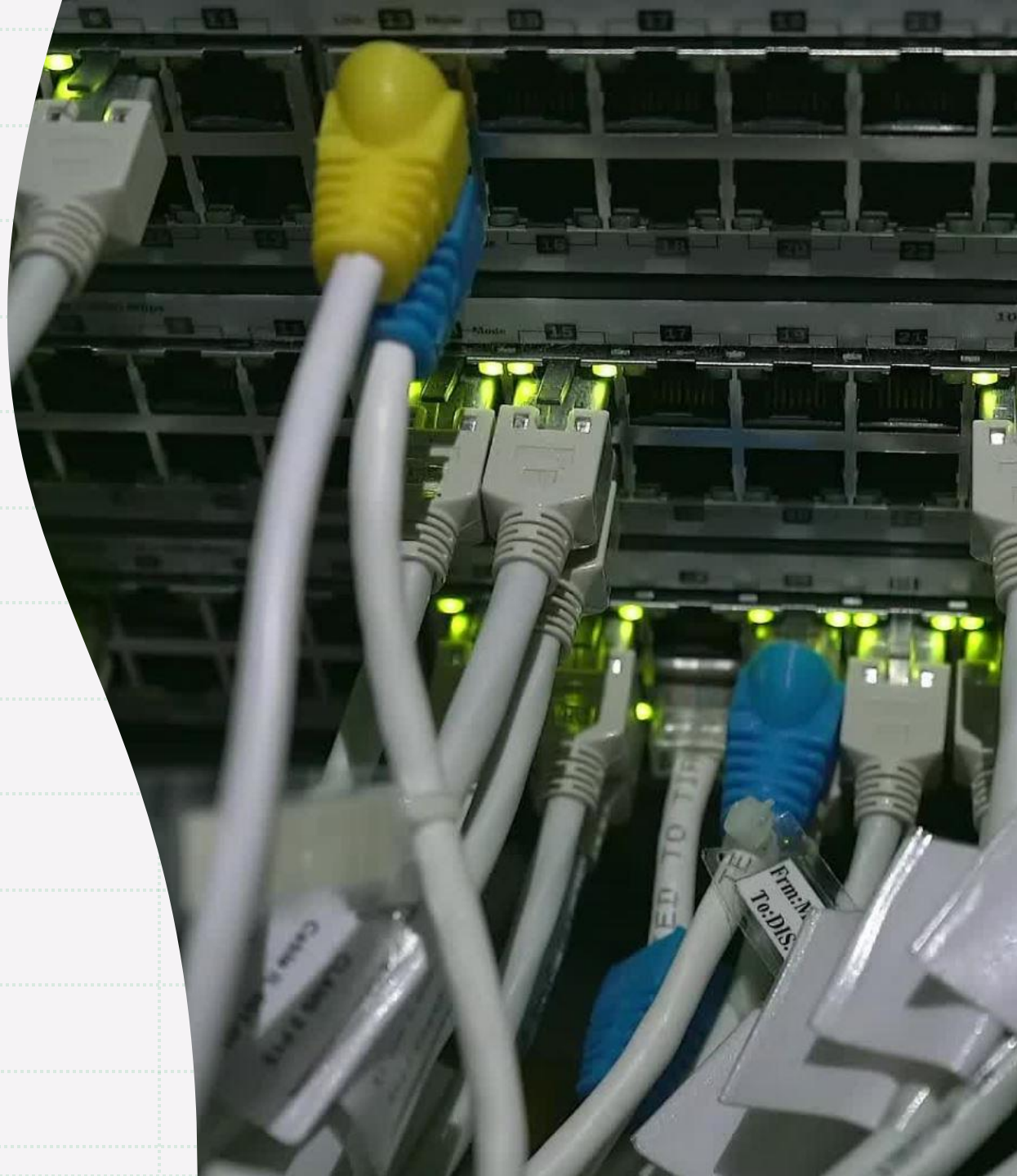


Privacy browsers

- **DuckDuckGo**
 - <https://duckduckgo.com/>
- **Opera**
 - <https://www.opera.com/>
- **TOR**
 - <https://www.torproject.org/>
 - TOR article
 - <https://www.vpnmentor.com/blog/tor-browser-work-relate-using-vpn/>

VPN

- A virtual private network is an encrypted connection over the Internet from a device to a network.
- <https://www.vpnmentor.com/blog/should-keep-vpn-on-at-all-times/>
- ExpressVPN
- ProtonVPN
- NordVPN
- IPVanish
- Surfshark



More security tools & options

- **Google now allows you to password protect your searches:**
 - <https://www.theverge.com/2021/5/24/22452122/google-my-activity-page-password-privacy-verification-web-and-app-history>
- **Privacy Badger - blocks invisible trackers**
 - <https://privacybadger.org/#What-is-a-third-party-tracker>
- **Tails is a portable operating system, hardened against attacks**
 - <https://tails.boum.org/>



GDPR compliant services:

check this list out



<https://gdpr.eu/compliant-services/>

- **Ghostery - blocks ads and trackers**
<https://www.ghostery.com/>
- **Signal - messaging, video, and calls without tracking.**
<https://signal.org/>
- **Privacy Pro SmartVPN - for ipads and other iOS**
<https://apps.apple.com/us/app/disconnect-privacy-pro-entire/id1057771839?ls=1>
- **Proton Email, VPN, Drive**
<https://protonmail.com/>

Other privacy pitfalls

Healthcare offices and hospitals

- Majority of attacks come from inside the organization
- 314,063,186 records exposed since 2009
- 94.6% of U.S. population
- <https://www.hipaajournal.com/health-care-data-breach-statistics/>





Why?

- Limited business knowledge
- Even less knowledge in security
- HIPAA provides minimal guidelines & requirements for financial privacy

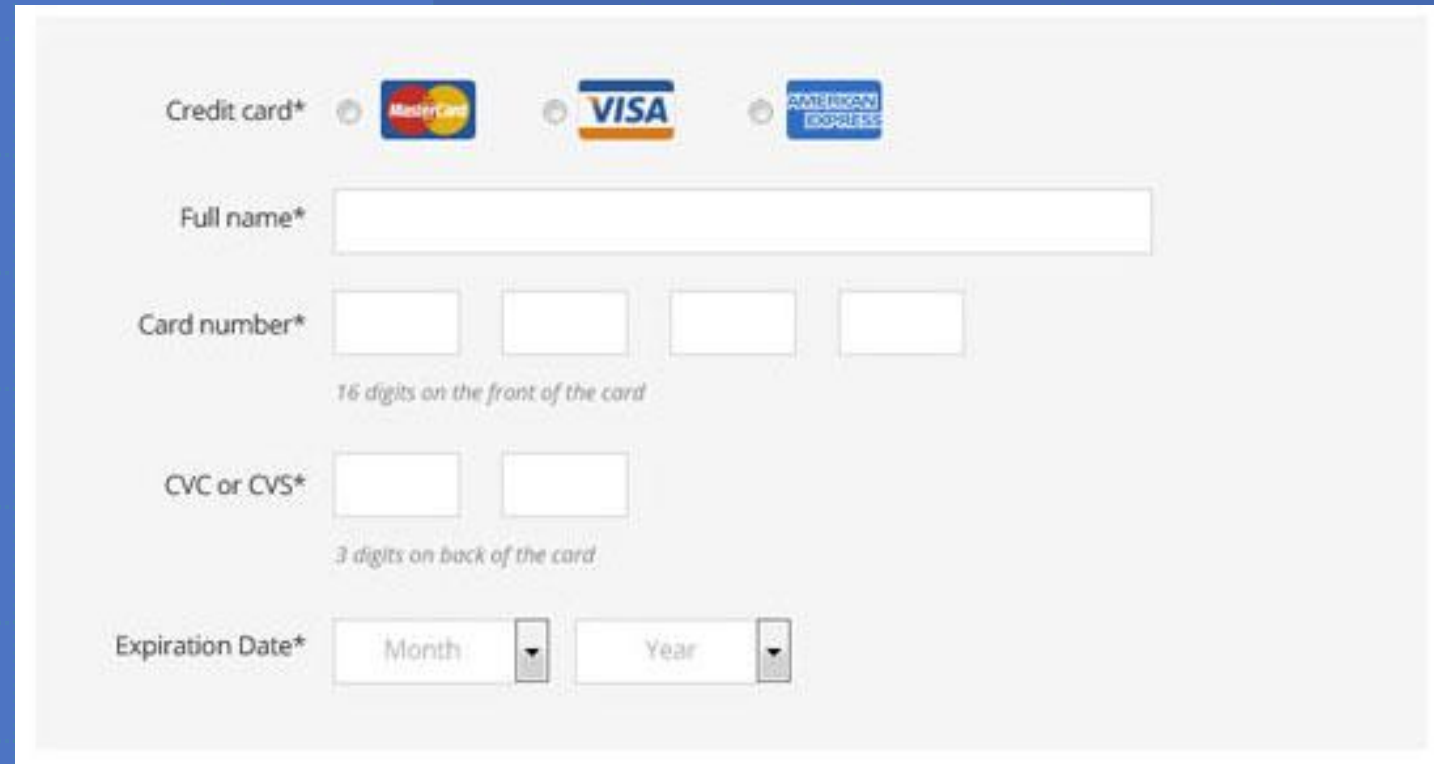
PCI DSS




Payment card industry
data security standards

<https://www.pcisecuritystandards.org/>

Reporting violations

- report directly to business
- report to credit card company



Credit card*   

Full name*

Card number*
16 digits on the front of the card

CVC or CVS*
3 digits on back of the card

Expiration Date* Month Year

PCI Data handling standards

- Do not keep physical copies
- NEVER store the CVV
- Store in a secure locked place
- Limit personnel with access
- Use security cameras in area
- Assess and securely destroy every 3 months
- Provide a privacy plan for clients

- **Significant fines and penalties:** If you are found to be incompetent, you will be subject to substantial non-compliance fines, regardless of the size of your company.
- **Legal costs, settlements, and judgments:** If your client's data has been compromised, he or she can sue, which can be extremely expensive. If you don't meet the PCI guidelines, credit card companies can take legal action against you, which may be more expensive.

<https://www.pcidssguide.com/what-are-the-pci-compliance-fines-and-penalties/>

What can I do?

- Use a pre-paid credit card
- Use a masked credit card
- 3rd party online vendors offers protections for both parties (ex. Plaid).
- **Never use a debit card!**



This Photo by Unknown author is licensed under CC BY-NC.

Masked Credit Cards

- Citibank
 - American Express
 - Capital One
-
- 1. Abine: Ironvest (Blur)
<https://www.abine.com/>
 - 2. Privacy.com: <https://privacy.com/>
 - 3. Revolut:
<https://www.revolut.com/en-US/>



This Photo by Unknown author is licensed under CC BY-SA.



The Internet of Things

Devices connected to each other and to a device or app that can control them. They generally connect through the Internet or Bluetooth.

Wearables

200-250 million

Benefits:

- Meeting your fitness goals
- Tracking your mental & physical health
- Providing warnings
- Convenience



Wearable concerns

- Tracking data and deletion of this data
- Location tracking
- Display can be read by others
- Audio and video recording without consent
- Little or no control over the data
- Lack of control over syncing with social media
- Health data is not covered by HIPAA



Regulations

- **2017 FTC**

- New safety measures: pins, patterns, automatic locking when distant from phone

- **2018 FTC**

- Warning letters to companies targeting children and not complying with COPPA (children's online privacy protection act)

- **2021 FTC**

- Devices that collect or use consumers' health information must comply with the Health Breach Notification Rule

Securing you smartwatch & fitness apps

- Secure your phone
- Run all updates (phone & fitness apps)
- Use an alias on fitness apps
- Check what data your fitness app is accessing
- Allow the most basic access (if possible)
- Make sure your apps use https
- Periodically check the accuracy of your data
- Enable theft deterrence settings
- Use vpn



Best and worst of the wearables

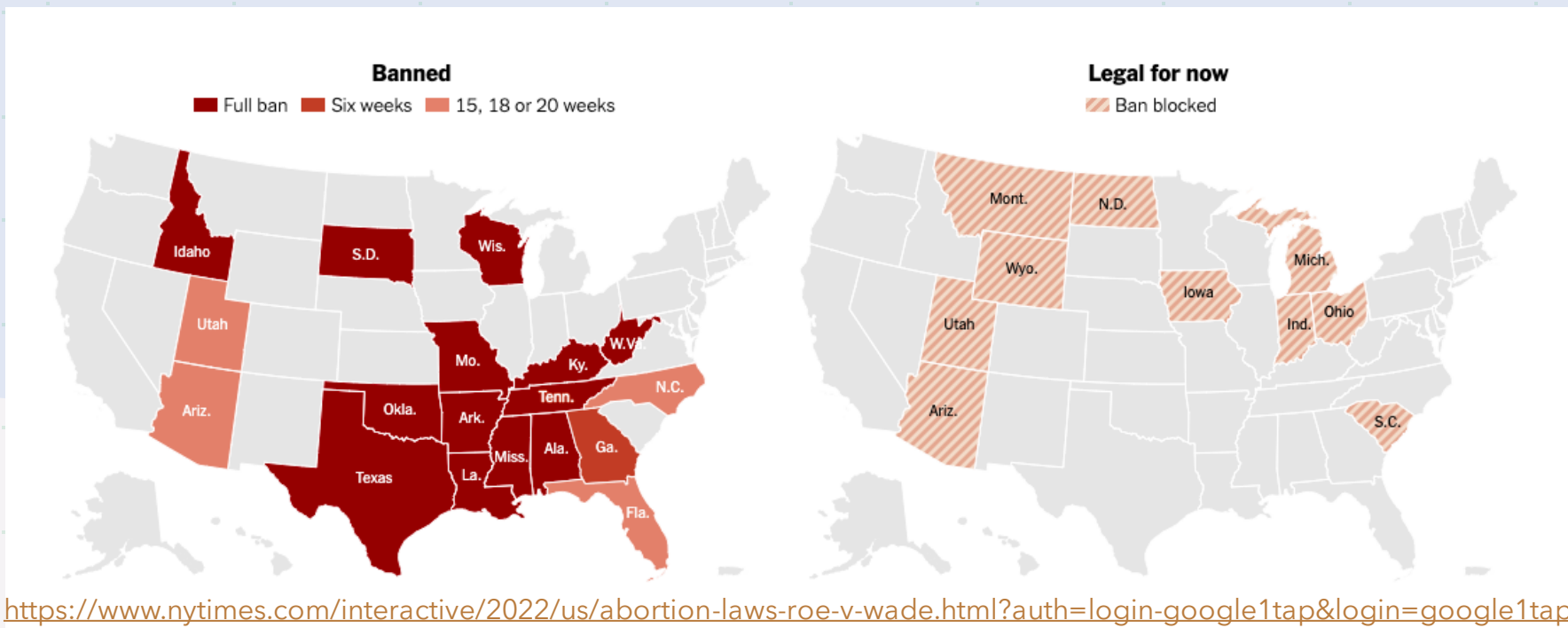
<https://foundation.mozilla.org/en/privacy-not-included/>

- **Best:**
 - Garmin
 - Apple Watch Series 6
- **Moderate:**
 - Fossil Gen 5
- **Worst:**
 - Fitbit; Ace, Versa 3, Sense
 - Samsung Galaxy Active 2, Watch 3
- **Don't even think about buying:**
 - Huawei products, Amazfit, MiBand & Amazon Halo

"The Supreme Court inadvertently kicked over the privacy hornet's nest," he said. "Anybody who cares about the right of privacy is going to be concerned, awakened, and I think activated by this wake-up call."

– Mark DiMassimo, founder and creative chief of creative agency DiGo.

Fertility & Period Trackers



Fertility and Period trackers

- Currently, these apps place the maternal health of women in danger in many states
- 87% of these apps share the data collected

Who knows if you are pregnant?

Health wearables:

- Fitbit (subpoenaed data)
- Oura

Smart Watches

Who else is tracking you?

Phone location

Virtual assistants

Smart cars

Shopping & marketing algorithms

Apps with upgraded security



This Photo by Unknown author is licensed under CC BY-SA-NC.

"In this scenario, we really don't have any data in readable form that we can submit to anyone," Sršen said. "In this form, data is also protected from theft, leak and users can be sure we are unable to share it or sell it to anyone." - Bellabeat

- **Bellabeat** implemented a private key encryption feature

<https://www.techtarget.com/searchcio/news/252522543/Womens-health-apps-enhance-data-privacy-after-Roe-v-Wade>

- **Flo** promised to protect user data and privacy:
 - stopped all sharing of data
 - introduced anonymous mode

Smart home

- Virtual assistants, doorbells, Smart TVs, appliances, thermostats, security cameras, smoke detectors
- Home insurers and utility companies have already made deals with Nest to put smart devices in their customers' homes



This Photo by Unknown author is licensed under [CC BY-SA](#).



Benefits

- Convenience!
- Home insurance discounts
- Ability to check in, receive alerts, and take care of the house while away
- Monitor energy use

General concerns

- **Limited user interfaces**
- **Device security limitations**
- **Lack of industry cybersecurity experience**
- **Lack of industry incentives**



The home network

- **Everything connected to your network can be hacked**
- **Smart devices are vulnerable to ransomware**
- Strong router password
- Limit devices on your network
- *Use a separate network for smart devices
- <https://www.androidauthority.com/smart-home-on-separate-wi-fi-3125772/>



Smart TVs: are they spying on you?

Yes!

- In 2019, the FBI issued a warning about smart TVs.
- Huawei products ALL have backdoors and should not be in your home!
- Samsung TVs record your conversations



This Photo by Unknown author is licensed under [CC BY-NC](#).

Smart TV basics

They have cameras (turn them off in settings or cover the camera eye)

Microphones (turn the tv off, don't leave in sleep mode)

They connect to your home network (use secure passwords for router)

They connect through 3rd parties, like Roku (always run all updates)



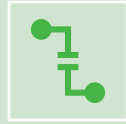
More ways to stay secure



Avoid accessing social media through the TV



Never access sensitive information through the TV



Disconnect the TV from the internet when not in use



Don't depend on the default security settings and passwords. Change the default password and check your settings.



Do a basic internet search with your model number and the words "microphone," "camera," and "privacy" to learn more.

Smart Speaker

- **General concerns:**

- Listening to us
- Recording us
- Sharing recordings of us



This Photo by Unknown author is licensed under [CC BY-SA-NC](#).

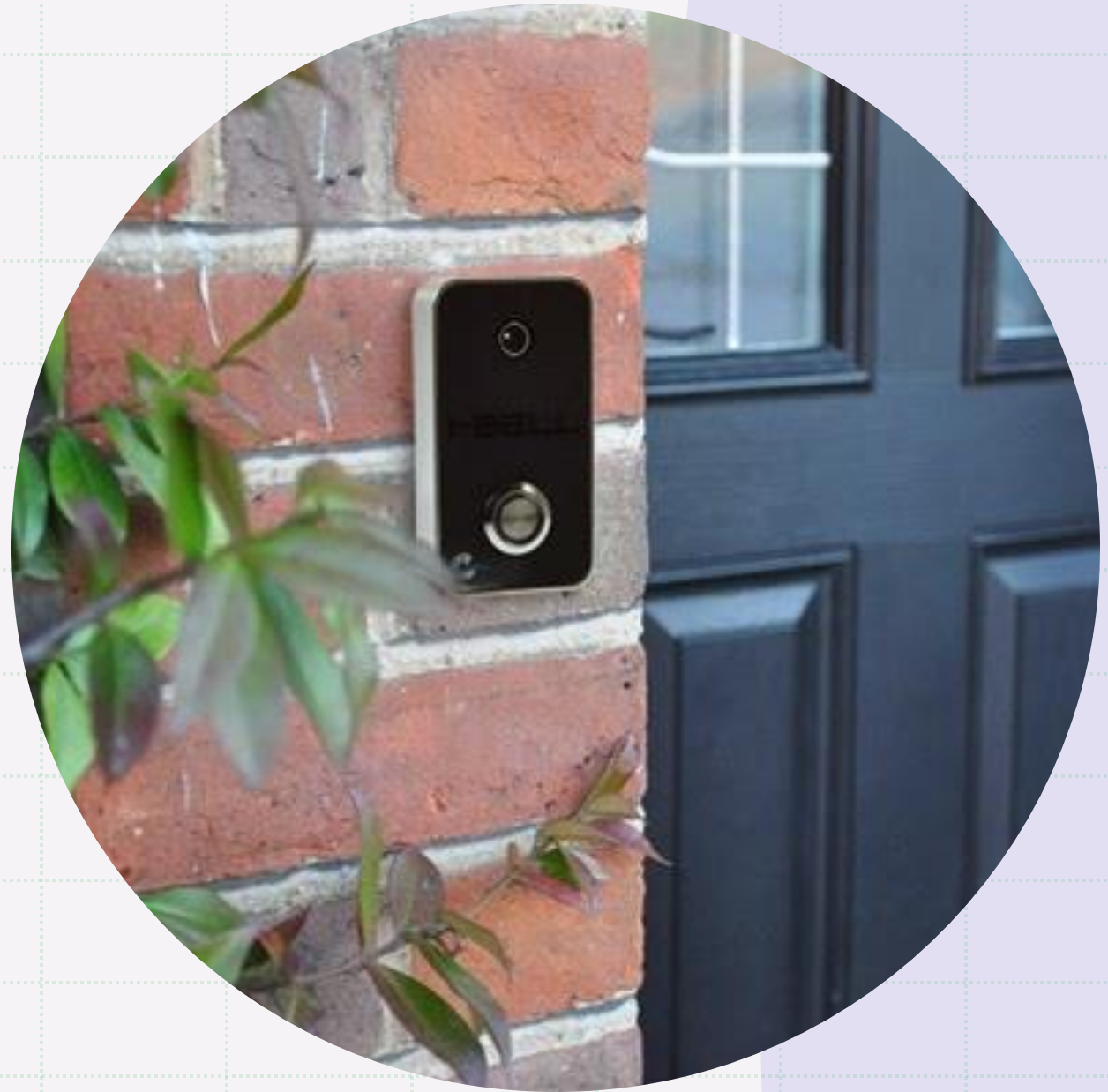
Staying secure

- ✓ **Enable the sound notification for when the device has been triggered and is listening (set to silent by default).**
- ✓ **Mute it when not in use**
- ✓ **Do not let children use unsupervised**
- ✓ **Opt out of human review of recordings**
- ✓ **Delete historical records (Amazon)**
 - ✓ <https://www.geekwire.com/2020/amazon-gives-customers-way-immediately-delete-alexa-voice-recordings-heres/>



The doorbell camera

Ring, Nest, and Arlo





This Photo by Unknown author is licensed under [CC BY-SA-NC](#).

Ring

Amazon company

Partners with 1,771 police departments, enabling police overreach

- **December 2021 - information between the app and the doorbell is still not encrypted**
- **Sending video to China**
- **The Neighbors app creates a surveillance state and encourages people to police their communities**
- **People have been able to hack into the doorbells and inside cameras**

Ring security improvements

- Now uses 2FA
- Employs end-to-end video encryption
- No longer allows police to contact Ring users
- Police can still post "requests for assistance" in the app

<https://www.cnet.com/home/security/rings-police-problem-didnt-go-away-it-just-got-more-transparent/>



Securing your doorbell

- Always use your own password
- Change your password regularly
- Use 2FA
- Use auto-update on devices and apps
- Delete recordings & related data
- If you have suspicions, turn it off!
- *strong wifi router password!



cars & appliances



This Photo by Unknown author is licensed under [CC BY-NC-ND](#).



This Photo by Unknown author is licensed under [CC BY-SA](#).

Risks & benefits of connected cars

- *"Modern cars are a privacy nightmare and it seems that the Fords, Audis, and Toyotas of the world have shifted their focus from selling cars to selling data."*
- --MISHA RYKOV, RESEARCHER @ *PRIVACY NOT INCLUDED
- <https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/#:~:text=then%20there's%20the%20devices%20you,you%20download%20the%20car's%20app>



Benefits of connected cars

1

Dealerships could automatically be notified of certain needs: tire rotation or oil change

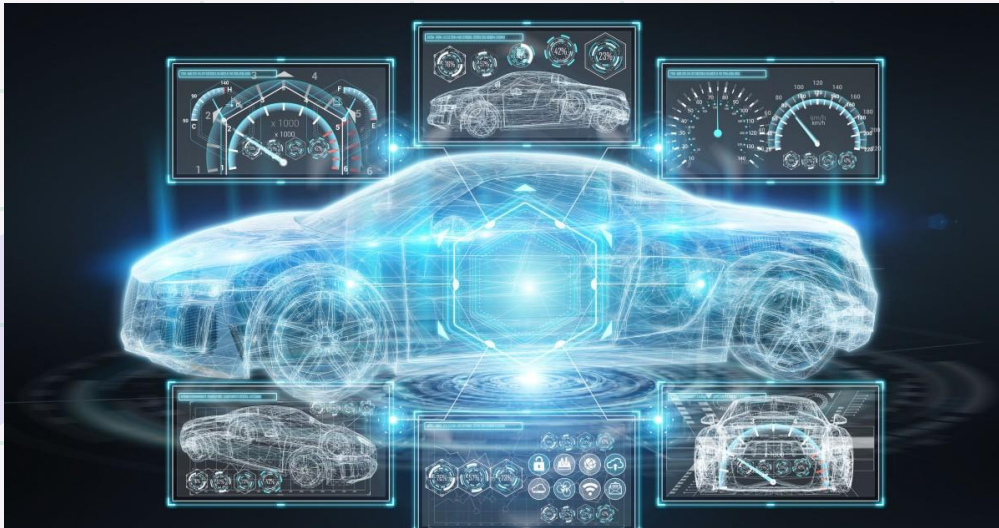
2

Insurance companies can lower costs based on driving habits (or raise them)

3

Help can be sent and your location shared automatically

Your car knows everything about you...



This Photo by Unknown author is licensed under [CCBY-SA](#).

Data Points:

- GPS (exact locations, when and where)
- Camera and video systems (gestures, travel routes, conditions inside and out)
- Audio recording (conversations)
- Connected phones (your contacts, text messages, etc.)
- Car apps: Audi, Tesla, Acura, Hyundai, BMW, Buick, Volvo, Cadillac, Chevrolet, Chrysler

Dystopian driving

- **Rental/selling cars:** delete your information through the infotainment center's paired devices list (use lighter port for charging).
- **Remote repossession**
- **Ford Motor Company 2021 patent:** ability to disable various systems for late payments or lock the car down except when driving to and from work.
- Ford has filed 2,045 patents from Jan. 1, 2023 to October 10, 2023

<https://arstechnica.com/cars/2023/03/ford-files-patent-for-system-that-could-remotely-repossess-a-car/#:~:text=Filed%20by%20Ford%2C%20the%20patent,t%20kept%20up%20with%20payments.>



Appliances

**Lack of interface
Lack of security
& privacy
experience**

At this time, most risks are largely related to mischievousness

Hackers may gain access your network

Thermostats may let police and thieves know when you are home

Power companies may want to control thermostats

*it all comes back to your router and passwords!

Resources

- Electronic Frontier Foundation: <https://www.eff.org/>
- CNET: <https://www.cnet.com/>
- Wired/security: <https://www.wired.com/category/security/>
- Terms of service <https://tosdr.org/>



Kelley Rowan
digital archives librarian

krowan@fiu.edu