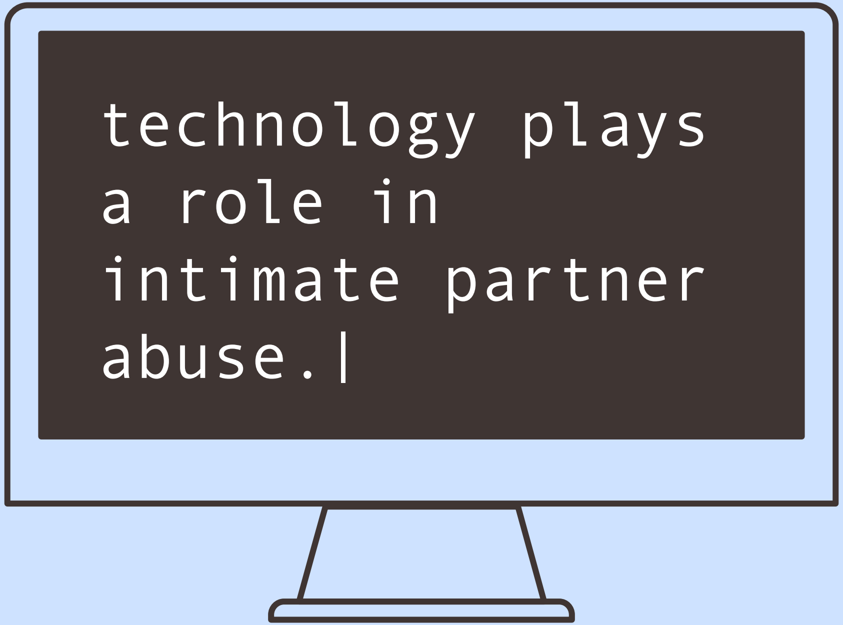
“It’s the Equivalent of Feeling Like You’re in Jail” Lessons from Firsthand and Secondhand Accounts of IoT-Enabled Intimate Partner Abuse

Sophie Stephenson, Majed Almansoori,
Pardis Emami-Naeini, and Rahul Chatterjee

WISCONSIN UNIVERSITY OF WISCONSIN–MADISON MADS&P Duke UNIVERSITY

harassing messages

non-consensual intimate imagery (NCII)



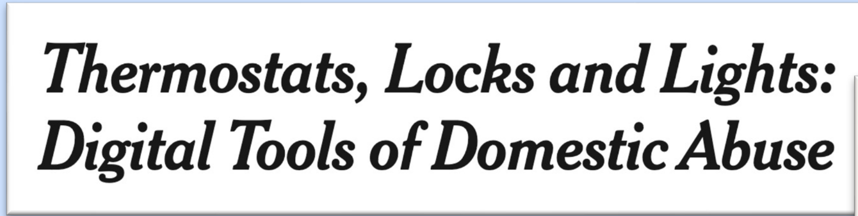
```
technology plays
a role in
intimate partner
abuse.|
```

surveillance

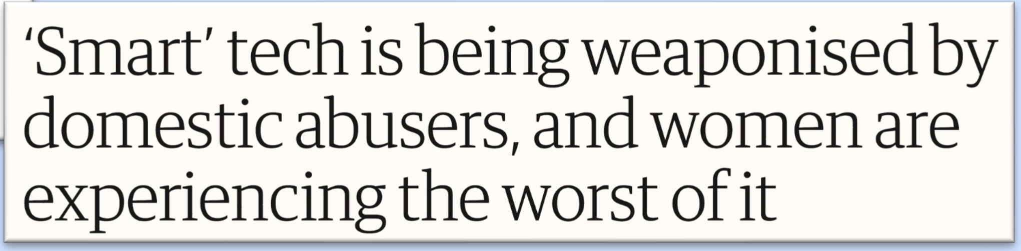
financial abuse

abuse with IoT devices

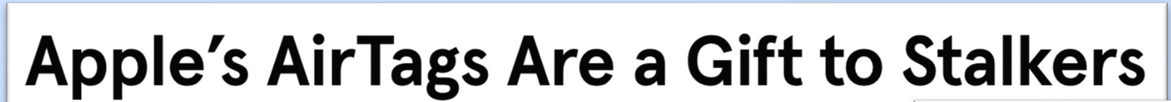
intimate partner abuse & IoT devices



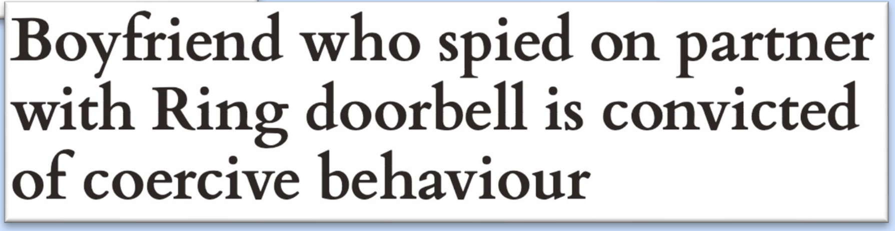
Thermostats, Locks and Lights: Digital Tools of Domestic Abuse



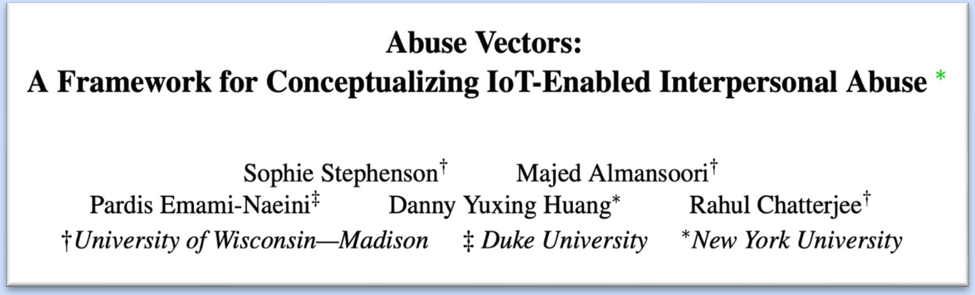
‘Smart’ tech is being weaponised by domestic abusers, and women are experiencing the worst of it



Apple’s AirTags Are a Gift to Stalkers



Boyfriend who spied on partner with Ring doorbell is convicted of coercive behaviour



Abuse Vectors:
A Framework for Conceptualizing IoT-Enabled Interpersonal Abuse *

Sophie Stephenson† Majed Almansoori†
Pardis Emami-Naeini‡ Danny Yuxing Huang* Rahul Chatterjee†
†*University of Wisconsin—Madison* ‡ *Duke University* **New York University*

[Bowles 2018] [Khan 2023]
[Cahn 2021] [Marsans 2023]

research questions

RQ1 How do survivors of intimate partner violence (IPV) **identify** this *IoT abuse*?

RQ2 How do survivors and advocates **mitigate** IoT abuse in IPV?

RQ3 Which **barriers** do survivors and advocates face along the way?

method: interviews (N = 20)

3

survivors

17

advocates

- 13 legal advocates
- 2 tech advocates
- 2 general advocates
- 4 leadership

150

years of experience

instances of IoT abuse in our interviews

# = 18	Audio & video surveillance	17	Location tracking
7	Disrupting the home environment	3	Tracking private data
2	Access restriction		

instances of IoT abuse in our interviews

= 18 Audio & video surveillance

17 Location tracking

7 Disrupti home e

private data

Most common abuse vector:
Covert Spying

2 Access restriction

instances of IoT abuse in our interviews

# = 18	Audio & video surveillance
17	Location tracking
7	Disrupting the home environment
3	Tracking private data
2	Access restriction

> *"With cameras, with the garage door, and the alarm system, all that, it's the equivalent of feeling like you're in jail."*

identifying IoT abuse in IPV

identifying IoT abuse

strategies

- Process of elimination
- Looking in device settings
- Searching for hidden spy devices
- Asking for help

identifying IoT abuse

strategies

- Process of elimination
- Looking in device settings
- Searching for hidden spy devices

for known devices

barriers

Devices do not indicate abuse

Devices are not seen as a threat

- Devices are discreet by design
- Reliance on manual inspection
- Hard to get peace of mind

> *“Does she know it was him? Does she have proof that it was him? No. But who else has that control?”*

identifying IoT abuse

strategies

- Process of elimination
- Looking in device settings
- Searching for hidden spy devices
- Asking for help

barriers

- Devices do not indicate abuse
- Devices are not seen as a threat

for hidden devices

Devices are discreet by design

Reliance on manual inspection

Hard to get peace of mind

identifying IoT abuse

strategies

- Process of elimination
- Looking in device settings

> *“A lot of times, they won’t find anything, and then the client doesn’t always feel like, ‘Oh, good, everything’s good now, they didn’t find anything.’ Like they still feel [...] that they are being watched."*

barriers

- Devices do not indicate abuse
- Devices are not seen as a threat
- Devices are discreet by design
- Reliance on manual inspection

Hard to get peace of mind

mitigating IoT abuse in IPV

mitigating IoT abuse

Device changes

Seeking help from outside services

Advocates' support strategies

Legal action

one overarching barrier

IoT abuse is not isolated

> *“ They’re trying to juggle personal* ***safety*** *and* ***work*** *and* ***leaving a relationship*** *and all these other things. And then I’m asking them to learn how to connect a router on top of it. ”*

mitigating IoT abuse: device changes

strategies

- Physical changes to device *(e.g., throwing it away)*
- Configuration changes *(e.g., revoking access)*

mitigating IoT abuse: device changes

strategies

- Physical changes to device *(e.g., throwing it away)*
- Configuration changes *(e.g., revoking access)*

barriers

- Abuser could notice changes
- Making changes is difficult
- Changes may be prohibited

> *"[It's] watching what you say and do in certain times, which sucks. But in some cases,* ***it's life or death*** *and that's what you have to do."*

mitigating IoT abuse: device changes

strategies

- Physical changes to device *(e.g., throwing it away)*
- Configuration changes *(e.g., revoking access)*

barriers

- Abuser could notice changes
- Making changes is difficult
- Changes may be prohibited

mitigating IoT abuse: legal action

strategies

- Seek physical protection *(e.g., via a restraining order)*
- Regain control of devices
- Seek legal charges *(e.g., for stalking)*

mitigating IoT abuse: legal action

strategies	barriers
- Seek protection *(e.g., via a restraining order)*	IoT abuse is not always [perceived] illegal in the US
- Regain control of devices	- US legal protections don't consider IoT devices
- Seek legal charges *(e.g., for stalking)*	

mitigating IoT abuse: legal action

strategies

- Seek protection
  (e.g., via a restraining order)
- Regain control of devices
- Seek legal charges
  (e.g., no-contact violation)

> *"If I get a restraining order, why shouldn't that apply to smart devices?"*

barriers

- IoT abuse is not always [perceived] illegal in the US

US legal protections don't consider IoT devices

towards removing barriers

five recommendations

Redesigning IoT devices

Training advocates & services

Creating tailored tools & services

Raising awareness

Collaborating with legal experts

“It’s the Equivalent of Feeling Like You’re in Jail” Lessons from Firsthand and Secondhand Accounts of IoT-Enabled Intimate Partner Abuse

Sophie Stephenson

sophie.stephenson@cs.wisc.edu

sophiestephenson.notion.site

WISCONSIN UNIVERSITY OF WISCONSIN–MADISON MAD S&P Duke UNIVERSITY

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, infographics & images by **Freepik**

References

- Nellie Bowles. Thermostats, locks and lights: Digital tools of domestic abuse. *The New York Times*, Jun 2018.
- Albert Fox Cahn and Eva Galperin. Apple's AirTags Are a Gift to Stalkers. *Wired*, May 2021.
- Coco Kahn. 'Smart' tech is being weaponised by domestic abusers, and women are experiencing the worst of it. *The Guardian*, April 2023.
- Isabella Marsan. Boyfriend who spied on partner with Ring doorbell is convicted of coercive behaviour. *Express*, April 2023.
- Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, Danny Yuxing Huang, and Rahul Chatterjee. Abuse Vectors: A Framework for Conceptualizing IoT-Enabled Interpersonal Abuse. *Proceedings of the 32nd USENIX Security Symposium*, August 2023.