Footprints to emissions: Exploring near-future digital vulnerabilities with creative methodologies

David A. Ellis [1], Iain Reid [2], Philip Wu [3], Asad Ali, Olivia Brown [1], Hannah Hutton[1]

[1] University of Bath
[2] University of Portsmouth
[3] Royal Holloway
[4] Ofcom

@davidaellis @Iain__Reid
@liv_brown20 @HJ_Hutton

Sprite+
Security, Privacy, Identity, Trust, Engagement, NetworkPlus

Background

- **Digital emissions** are traces of seemingly innocuous data that reflect everyday activities (e.g., liking a Tweet). However, they are also essential for the modern economy (e.g., financial transactions).

- Like greenhouse gases, digital emissions are invisible and appear harmless, but can make individuals, groups, and society vulnerable.

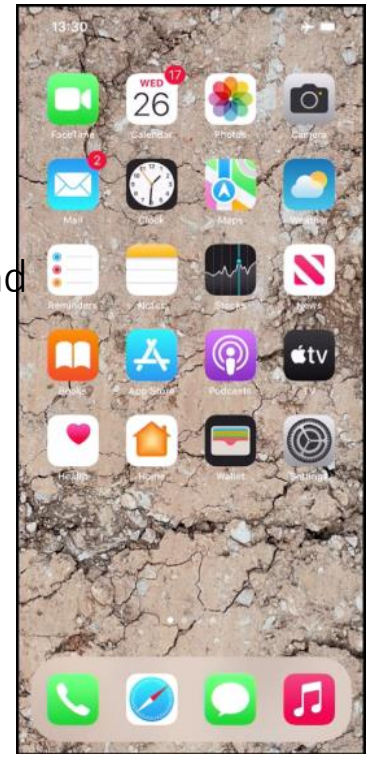
- As more systems become interconnected and new devices enter the digital ecosystem, the problem of digital emissions and how to manage pollution will become of paramount importance in the next 5-10 years.

- For citizens to become proactive rather than reactionary in protecting their data, we need to first evaluate **how people understand digital emissions and associated vulnerabilities in their everyday use of digital devices.**

(Credit: Louis Netter)

Methods

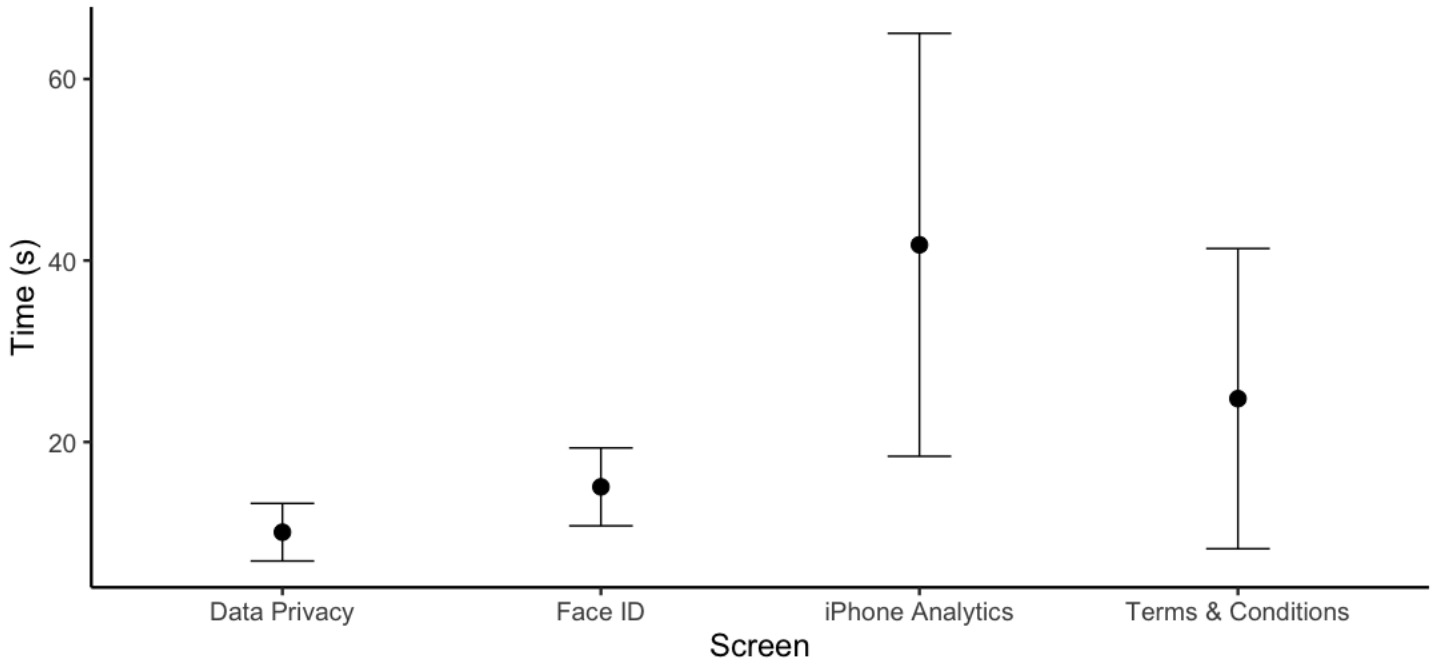
We tested how **probe-based methods** can help elicit reactions and reflections about everyday and speculative scenarios for current and near-future digital vulnerabilities from digital emissions.



Phase	N	Method	Procedure
Phase 1: Part A	20	Concurrent think-aloud protocols and interview probes	Participants walk the researcher through their own smartphone privacy set-up and associated interactions/apps.
Phase 1: Part B	20	Concurrent think-aloud protocols and interview probes	Participants set up a new smartphone from scratch and explain privacy-related decisions
Phase 2	25	Focus groups	Participants discuss fictitious scenarios in comics specifically created for the study

(Credit: Louis Netter)

Quant


60
40
20
Time (s)
Data Privacy
Face ID
iPhone Analytics
Terms & Conditions
Screen


10:30
Back
iPhone Analytics
Help Apple improve its products and services by allowing analytics of usage data from your iPhone. You can change your decision later in Settings.
All data is collected using privacy preserving techniques such as differential privacy and is not associated with you or your account.
About Device Analytics & Privacy...
Share with Apple
Don't Share

Qual

College educated young people are aware of a broad range of risks associated with using digital technologies, from privacy risks in omnipresent tracking cookies to security risks such as hacking and identify theft. This finding is in line with the extant literature.

Some participants in the study went to great lengths to manage their digital footprint: they regularly clean up their Internet history, use VPN, and even create “burner” accounts to avoid tracking and spamming.

Participants care much more about their smartphone device than their digital footprint. They would ‘panic’ if someone stole their phone because the phone is such an important artefact integral to their daily life, losing it means ‘massive inconvenience’; by contrast, stolen data is ‘not a disaster’ because the data are either recoverable from cloud backup or not viewed as especially sensitive.

Lastly, there is an ambivalence towards information security risks among young people. Some participants were struggling to make sense of digital risks (what do they mean in more concrete terms?), which highlights the need to enhance infosec education among young people.

I guess we are not really made aware of the dangers of like data misuse, so I wouldn't know what to think first if like they said oh your data has been stolen, I would think well what does that mean?

Nevertheless, there are two contrasting reactions toward the hypothetical scenario of stolen personal data: one group would 'feel exposed', while the other shrugs off any potential consequences by saying 'there's nothing really private'.

The latter group is particularly interesting. The notion of the privacy paradox builds upon the observation that people care about their privacy but act as if they don't; however, our finding seems to suggest there is no such 'paradox' or discrepancy between attitude and behaviour among some young people. This aligns with recent work that has provided further evidence against the privacy paradox.

Exploring User Motivations Behind iOS App Tracking Transparency Decisions

Hannah J Hutton
hjh53@bath.ac.uk
University of Bath
Bath, United Kingdom

David A Ellis
dae30@bath.ac.uk
University of Bath
Bath, United Kingdom

ABSTRACT

Apple's App Tracking Transparency framework allows users to decide whether they want to allow their activity to be tracked for advertising purposes. In this work we examine the tracking decisions made by 312 participants and their associations with privacy concern and personality factors, and conduct a thematic analysis on participants' reasons for choosing to accept or reject tracking requests. Despite 51% of participants reporting that they had rejected tracking for privacy reasons, higher privacy concern scores did not correlate with a lower rate of tracking acceptance. Additionally, 43% of participants held incorrect beliefs about what tracking does, including nearly a quarter who mistakenly believed that accepting a tracking request would share their location with the requesting app. We suggest explanations for these misconceptions and provide recommendations that may improve usability of both App Tracking Transparency and future Privacy Enhancing Technologies.

CCS CONCEPTS

• **Human-centered computing** → **Empirical studies in ubiquitous and mobile computing**; • **Information systems** → **Online advertising**; • **Security and privacy** → **Human and societal aspects of security and privacy**; *Social aspects of security and privacy*; *Privacy protections.*

KEYWORDS

App Tracking Transparency, Apple, iOS, privacy, privacy concern, privacy paradox, privacy calculus, privacy salience, privacy decision making

ACM Reference Format:
Hannah J Hutton and David A Ellis. 2023. Exploring User Motivations Behind iOS App Tracking Transparency Decisions. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23), April 23–28, 2023, Hamburg, Germany.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3544548.3580654

screen. Whilst some users might be concerned about protecting sensitive information such as their banking details or passwords, even seemingly innocuous data such as the number of times a smartphone is picked up in a day can be used to identify individuals from a group [35]. Other data such as social media interactions can be used to build up a profile of a user which can be used for recommending relevant content, for targeted advertising, or for something more sinister as seen in the Cambridge Analytica scandal. In this case, millions of US voters were subject to targeted advertising which is alleged to have influenced the outcome of the 2016 US election [42]. The practice of 'tracking' these types of behavioural data is common across both iOS and Android ecosystems to identify interests and personalise ads. Privacy controls are therefore critical for allowing users to decide and enforce how much information they are willing to share, and with whom.

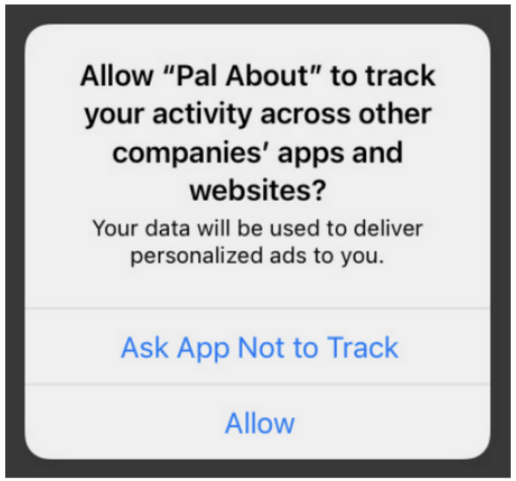
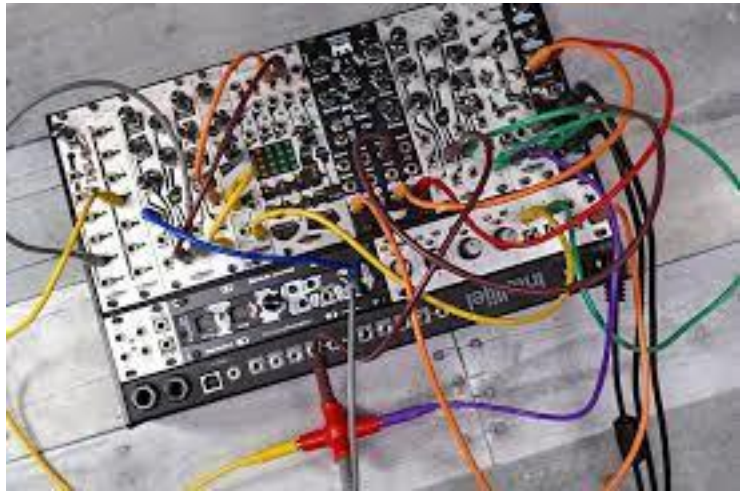


Figure 1: An example tracking request

Impacts/Next Steps

(Credit: Louis Netter)



Footprints to emissions: Exploring near-future digital vulnerabilities with creative methodologies

David A. Ellis [1], Iain Reid [2], Philip Wu [3], Asad Ali, Olivia Brown [1], Hannah Hutton[1]

[1] University of Bath
[2] University of Portsmouth
[3] Royal Holloway
[4] Ofcom

@davidaellis @Iain__Reid
@liv_brown20 @HJ_Hutton

Sprite+
Security, Privacy, Identity, Trust, Engagement, NetworkPlus