University of BRISTOL | UCL | KING'S College LONDON | THE UNIVERSITY of EDINBURGH | UNIVERSITY OF BATH

REPHRAIN

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

@REPHRAIN1

Professor Awais Rashid – Director
University of Bristol

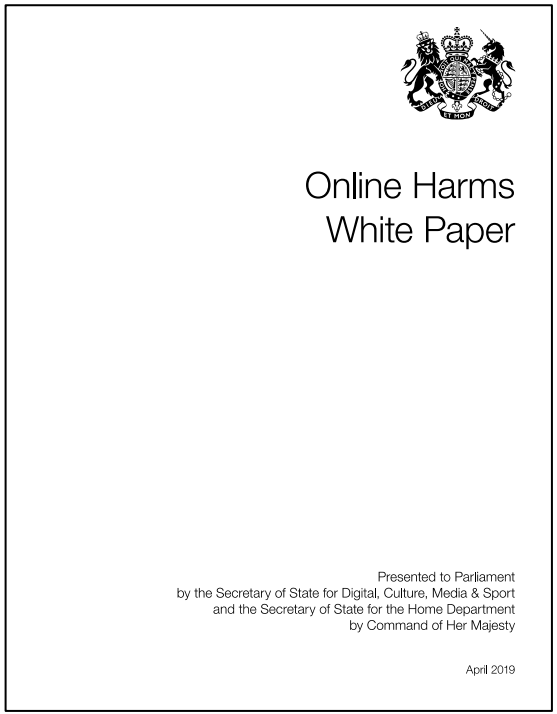
bristol.ac.uk

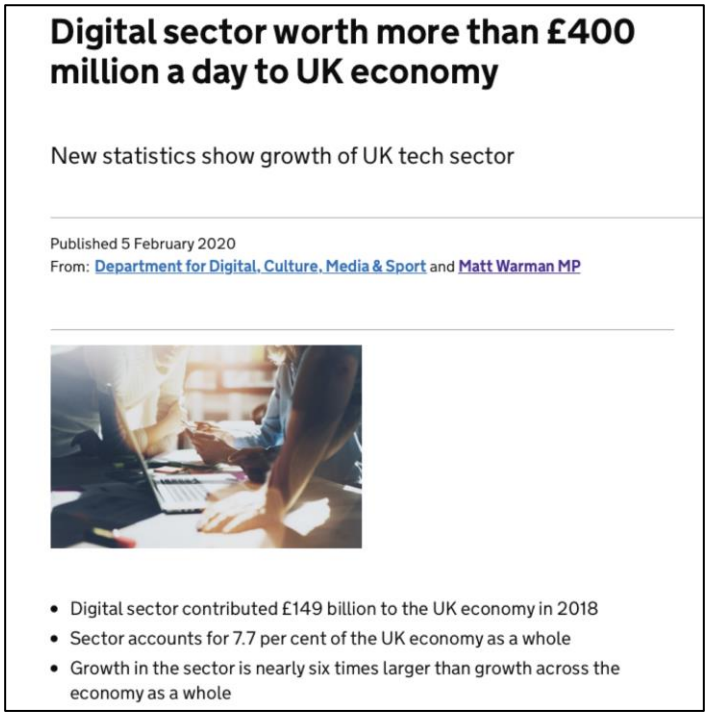
UK Research and Innovation

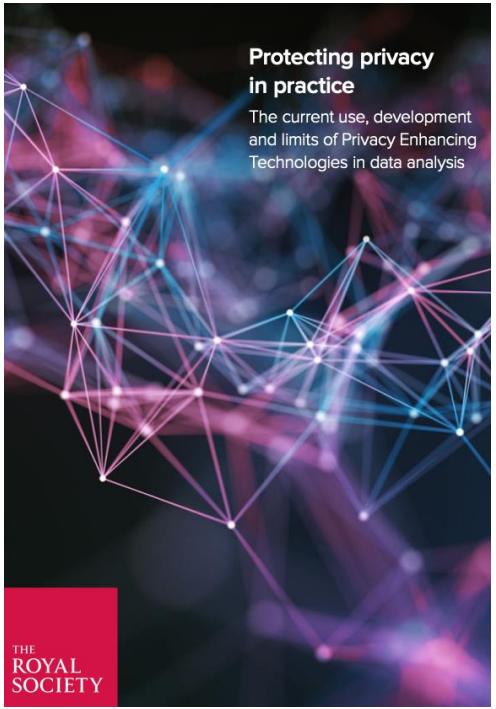
National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

The Context

REPHRAIN
Protecting citizens online







bristol.ac.uk

Support The Guardian
Available for everyone, funded by readers
Contribute → Subscribe →

Search jobs | Sign in | Search | The Guardian | UK edition

News | Opinion | Sport | Culture | Lifestyle | More

UK World Business Coronavirus Football Environment UK politics Education Society Science Tech Global development Obituaries

The Observer
Smart homes

How to stop your smart home spying on you

Everything in your smart home, from the lightbulbs to the thermostat, could be recording you or collecting data about you. What can you do to curb this intrusion?

Davey Winder
Sun 8 Mar 2020 13.00 GMT

820 833

Illustration and animation by James Melaugh

BBC | BBC Account | Home | News | Sport | Weather | iPlayer | Sound

NEWS

Home | Coronavirus | US Election | UK | World | Business | Politics | Tech | Science | Health | Family & Education

Technology

Amazon's Ring logs every doorbell press and app action

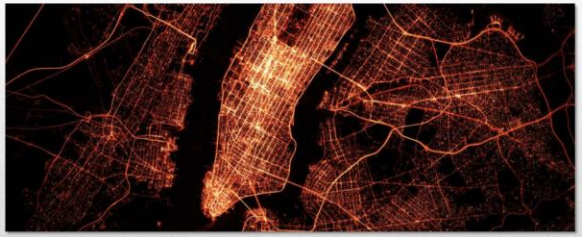
By Leo Kelion
Technology desk editor

4 March

The Ring doorbells use both cameras and motion sensors to detect when someone approaches

Amazon keeps records of every motion detected by its Ring doorbells, as well as the exact time they are logged down to the millisecond.

NYT App Articles

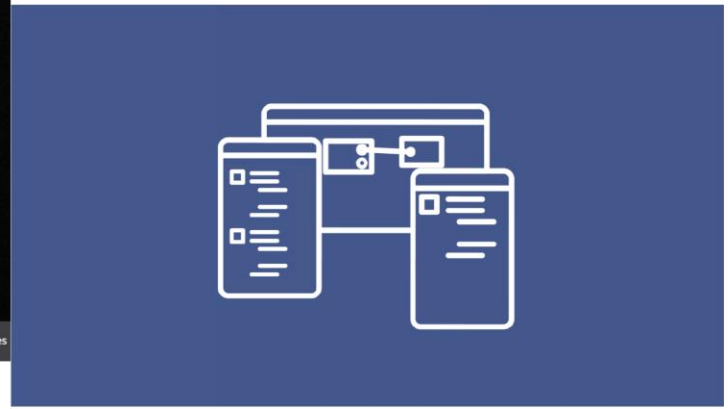


Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret

@jenvalentino jennifer.valentino@nytimes.com

April 16, 2018

Hard Questions: What Data Does Facebook Collect When I'm Not Using Facebook, and Why?



Hard Questions is a series from Facebook that addresses the impact of our products on society.

By David Baser, Product Management Director

Opinion | THE PRIVACY PROJECT

We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.

By Kevin Litman-Navarro

In the background here are several privacy policies from major tech and media platforms. Like most privacy policies, they're verbose and full of legal jargon — and opaquely establish companies' justifications for collecting and selling your data. The data market has become the engine of the internet, and these privacy policies we agree to but don't fully understand help fuel it.

Privacy settings

Please manage your cookie choices by switching the consent toggles on or off under the Purposes listed below. You can also choose to click:

Reject all Accept all

Purposes | Features | Site Vendors

Purposes

User Consent | Legitimate Interest

Purposes

We have a need to use your data for this processing purpose that is required for us to deliver services to you.

Personalised ads and content, ad and content measurement, audience insights and product development

Status: Accepted All Off On

Special Purposes

We use your data for these purposes so we

Match and combine offline data sources

Vendors can:

- Combine data obtained offline with data collected online in support of one or more Purposes or Special Purposes.

VEXPRO TECHNOLOGIES LTD, Permodo GmbH, BeeswaxIO Corporation, Bombora Inc., RevJet, Publicis Media GmbH, Digiseg ApS, EASYmedia GmbH, IPONWEB GmbH, Signals (Next14 Group), Sonobi, Inc, Blis Media Limited, xAd, Inc. dba GroundTruth, Unruly Group Ltd, BIDSWITCH GmbH, Inspired Mobile Limited, Near Pte Ltd, INFINIA MOBILE S.L., AdTheorent, Inc, Deutsche Post AG, Location Sciences AI Ltd., StackAdapt, Dugout Limited, TabMo SAS, Codewise VL Sp. z o.o. Sp. k, comScore, Inc., Free Stream Media Corp. dba Samba TV, Yieldlab AG, Sizmek by Amazon, InMobi Pte Ltd, Targetspot Belgium SPRL

Link different devices

Vendors can:

- Deterministically determine that two or more devices belong to the same user or household
- Probabilistically determine that two or more devices belong to the same user or household
- Actively scan device characteristics for identification for probabilistic identification if users have allowed vendors to actively scan device characteristics for identification (Special Feature 2)

VEXPRO TECHNOLOGIES LTD, PROXISTORE, Permodo GmbH, Blue, Publicis Media GmbH, EASYmedia GmbH, IPONWEB GmbH, Signals (Next14 Group), Blis Media Limited, xAd, Inc. dba GroundTruth, Unruly Group Ltd, Ad Alliance GmbH, Inspired Mobile Limited, Near Pte Ltd, INFINIA MOBILE S.L., AdTheorent, Inc, StackAdapt, : Tappx, Dugout Limited, TabMo SAS, Codewise VL Sp. z o.o. Sp. k, comScore, Inc., Free Stream Media Corp. dba Samba TV, Yieldlab AG, Sizmek by Amazon, InMobi Pte Ltd, Targetspot Belgium SPRL, Mediasmart Mobile S.L., travel audience GmbH, Telaria SAS, Epsilon, Fifty Technology Limited, LiveRamp, Inc., Adzymic Pte Ltd

Receive and use automatically-sent device characteristics for identification

Vendors can:

- Create an identifier using data collected automatically from a device for specific characteristics, e.g. IP address, user-agent string.
- Use such an identifier to attempt to re-identify a device.

Vendors cannot:

- Create an identifier using data collected via actively scanning a device for specific characteristics, e.g. installed font or screen resolution without users' separate opt-in to actively scanning device characteristics for identification.
- Use such an identifier to re-identify a device.

VEXPRO TECHNOLOGIES LTD, BeeswaxIO Corporation, Bombora Inc., Blue, EASYmedia GmbH, IPONWEB GmbH, Signals (Next14 Group), Blis Media Limited, xAd, Inc. dba GroundTruth, Market Resource Partners LLC, Unruly Group Ltd, BIDSWITCH GmbH, GumGum, Inc., Inspired Mobile Limited, INFINIA MOBILE S.L., AdTheorent, Inc, Adobe Advertising Cloud, Index Exchange, Inc., Smart Adserver, Effiliation, Dugout Limited, Axel Springer Teaser Ad GmbH, TabMo SAS, Venatus Media Limited, Codewise VL Sp. z o.o. Sp. k

The Observer
Apps

Internet privacy: the apps that protect you from your apps

Worried about the data collected about you? A new generation of startups is making apps to put your privacy settings straight

Alex Hern
@alexhern
Sun 16 Feb 2020 07.00 GMT

344 282

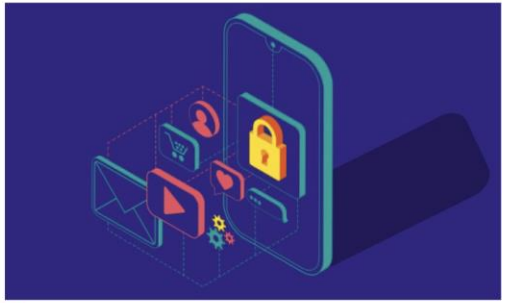


Illustration: James Melaugh/The Observer

bristol.a

BBC | BBC Account | Home | News | Sport | Weather | iP

NEWS

Home | Coronavirus | US Election | UK | World | Business | Politics | Tech | Science | Heal

Technology

Coronavirus: YouTube tightens rules after David Icke 5G interview

By Leo Kelion
Technology desk editor

7 April

Coronavirus pandemic

A lengthy interview with David Icke was live-streamed on YouTube on Monday

YouTube has banned all conspiracy theory videos falsely linking coronavirus symptoms to 5G networks.

Support The Guardian
Available for everyone, funded by readers
Contribute → Subscribe →

Search jobs | Sign in | Search | UK edition

The Guardian

News | Opinion | Sport | Culture | Lifestyle | More

World ▸ Europe US Americas Asia Australia Middle East Africa Inequality Global development

Coronavirus: 100 days that changed the world
Coronavirus

Julia Carrie Wong

Tech giants struggle to stem 'infodemic' of false coronavirus claims

sive intervention and have embraced official
y via Getty Images

esearch reveals vast

BBC | BBC Account | Home | News | Sport | Weather | iPlayer | Sounds

NEWS

Home | Coronavirus | US Election | UK | World | Business | Politics | Tech | Science | Health | Family & Education

Flat Earth: How did YouTube help spread a conspiracy theory?

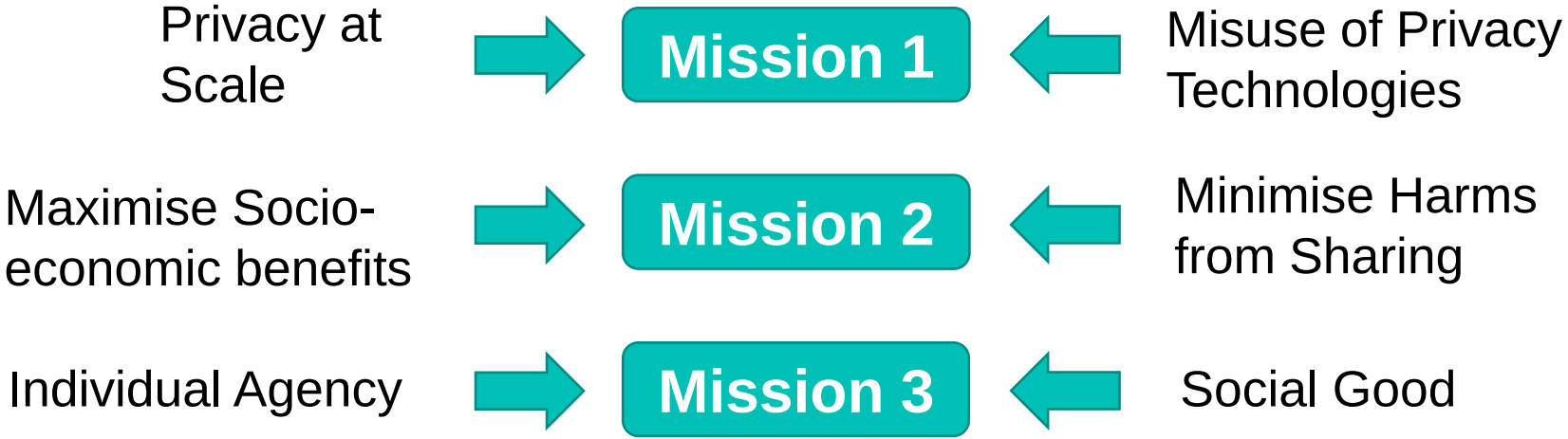
All around the world, there are conspiracy theorists who believe the Earth is flat. And their

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

REPHRAIN Missions

REPHRAIN
Protecting citizens online

Address the fundamental tensions and imbalances pertaining to protecting citizens online



Burges Salmon

Center for the Cultivation of Technology

CYBSAFE

digi.me

OneSpan

GENIES

Google

GOV.UK

HARVARD LAW SCHOOL

hazy

THE HEALTH DATA EXCHANGE
Share your data for faster cures

KU LEUVEN

NCA
National Crime Agency

CMA
Competition & Markets Authority

ORG OPEN RIGHTS GROUP

POLITIE

PRIVITAR

METROPOLITAN POLICE

Tor

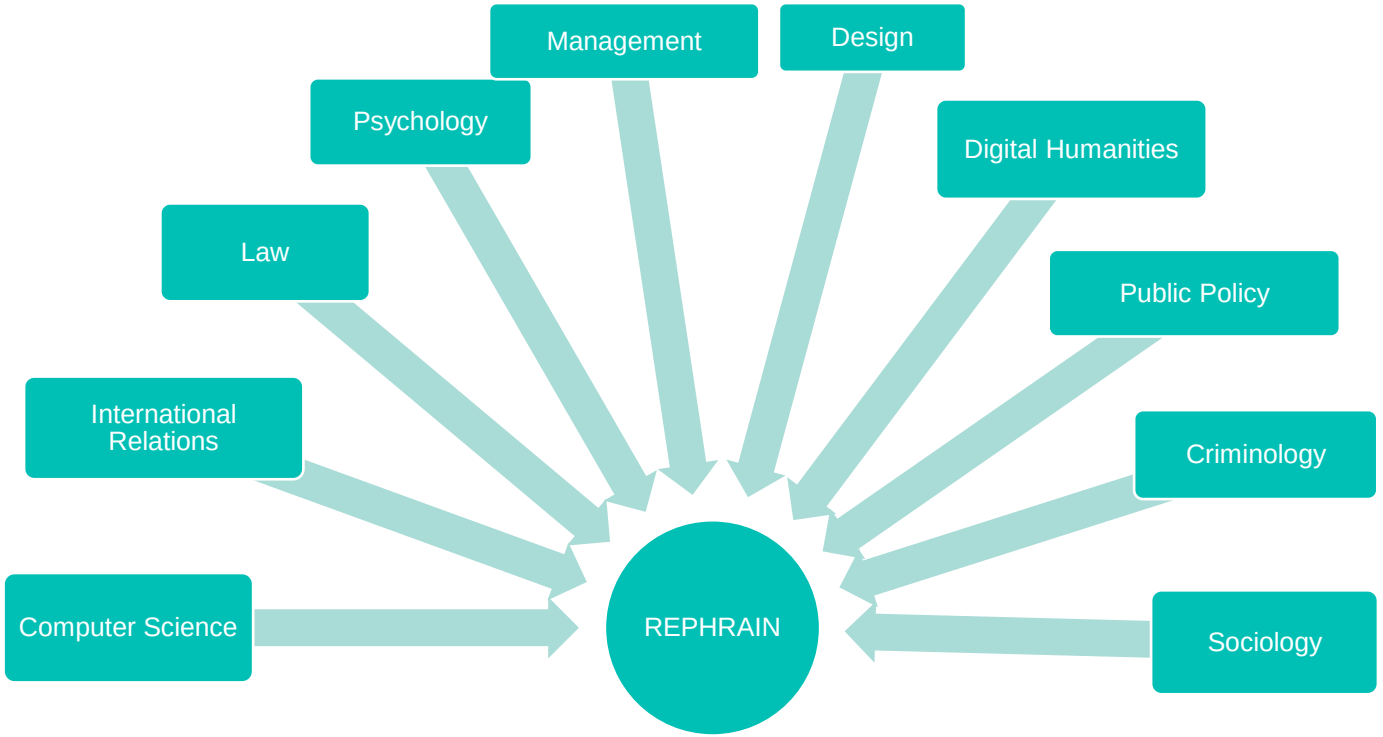
UKAuthority

VUB VRIJE UNIVERSITEIT BRUSSEL

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

Building National Capability

REPHRAIN
Protecting citizens online

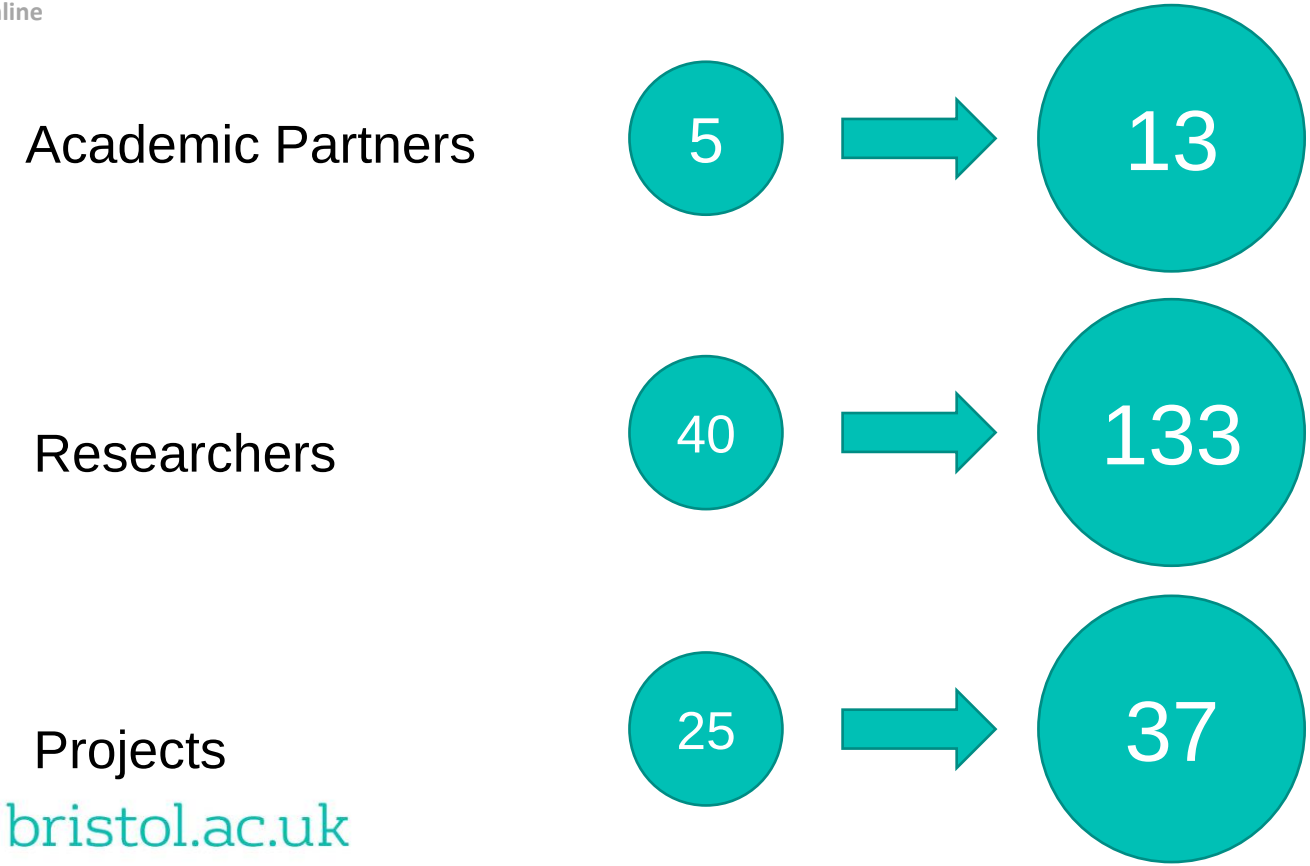


bristol.ac.uk

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

Building National Capability

REPHRAIN
Protecting citizens online



£900K new projects

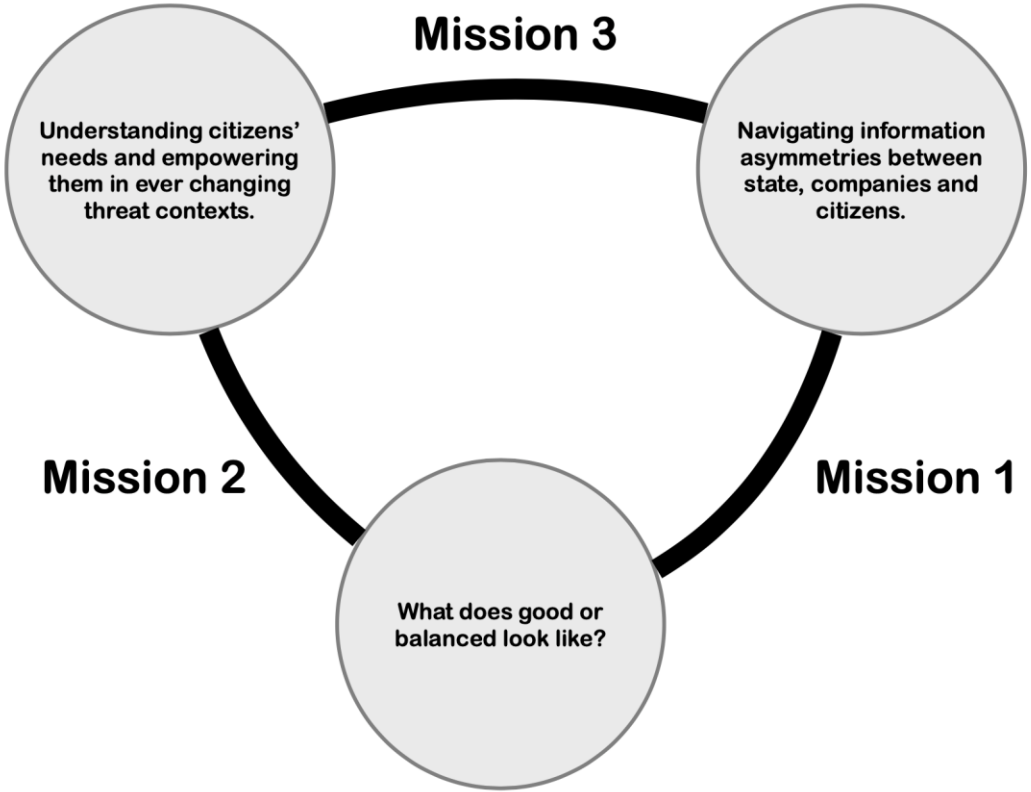
bristol.ac.uk

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

Building National Capability

REPHRAIN
Protecting citizens online

Scoping work to inform the £11M UKRI call on complementary node projects as part of the Protecting Citizens Online Strategic Priority Fund



bristol.ac.uk

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

Building National Capability

REPHRAIN
Protecting citizens online

AP4L	Protecting online privacy for people going through serious life events
3PO	Protecting public-facing professionals and their dependants online
PRIME	Addresses concerns that the digitalisation of key government services may lead to existing inequalities being reproduced or exacerbated
AGENCY	Addresses harms that arise from a complex interaction of societal processes driven by diverse stakeholders

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

Fundamental Research

REPHRAIN
Protecting citizens online

CLARITI – MuMiN: A Large-Scale Multilingual Multimodal Fact-Checked Misinformation Social Network Dataset

PI – Ryan McConville, RA – Dan Saattrup Nielsen

A multimodal machine learning based study of misinformation on social networks in the form of text, videos and rich structural connectivity

MuMiN Dataset

21 million tweets belonging to *26K threads*

Linked to 13K fact-checked claims

in 41 languages

Publicly Available:
https://mumin-dataset.github.io/

bristol.ac.uk

Fundamental Research

The applicability of the UK Computer Misuse Act 1990 for cased of technology-enabled domestic violence and abuse (Tech Abuse)

PI – Leonie Tanczer, RA – Francesca Stevens

Court cases in England and Wales where either tech-abuse was involved or was suspected in an intimate partner violence (IPV) context

Tech abuse continues to be **prevalent and common** within the analysed domestic abuse court cases

CMA 1990 applicable to unauthorised access to mobile phone messages and social media accounts, and manipulation of partner's social media account

Fundamental Research

FAIRCROWD - Fair Private and Distributed Evaluation of Crowd-sourced user data

PI – Rik Sakar and Tariq Elahi, RA – Hao Tsung Yang

Modern businesses depend on personal data to improve machine learning and data driven decision making

Contributors knowing value of their data can enable better data markets and reduce privacy risks

Shapley Values algorithm developed for privacy-preserving data valuation – uses substantially less data and is differentially private

Fundamental Research

Query - Efficiently Querying User Sequences While Preventing Their Reconstruction

PI – Grigorios Loukides, RA – Huiping Chen

Strings (sequences of elements) can model location or genetic information, purchases of products online, or natural language.

A popular type of queries: Is a given length-k string part of the string S we indexed? However, such queries allow an attacker to (reconstruct) S.

Construct a data structure to prevent the reconstruction attack with high probability while storing as many answers to useful queries as possible.

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

Fundamental Research

REPHRAIN
Protecting citizens online

Defining harm, mapping tech interactions associated with harm and understanding/auditing mitigation strategies

PI – Adam Joinson, Laura Smith, Danae Stanton Fraser, David Elli, RA – Alicia Cork, Othman Esoul

Developed psychological model of contextual vulnerability online

Studies with Genies users to assess the risks of digital fashions NFTs

Ecological momentary assessment study on everyday experiences of harm

Studies on simulated social media platform for assessing how sociopsychological context impacts vulnerability to radical ideas

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

Co-Producing Artefacts

REPHRAIN
Protecting citizens online

Design & Engagement

Adoption & Adoptability

Responsible, Inclusive & Ethical Innovation

Policy & Regulation

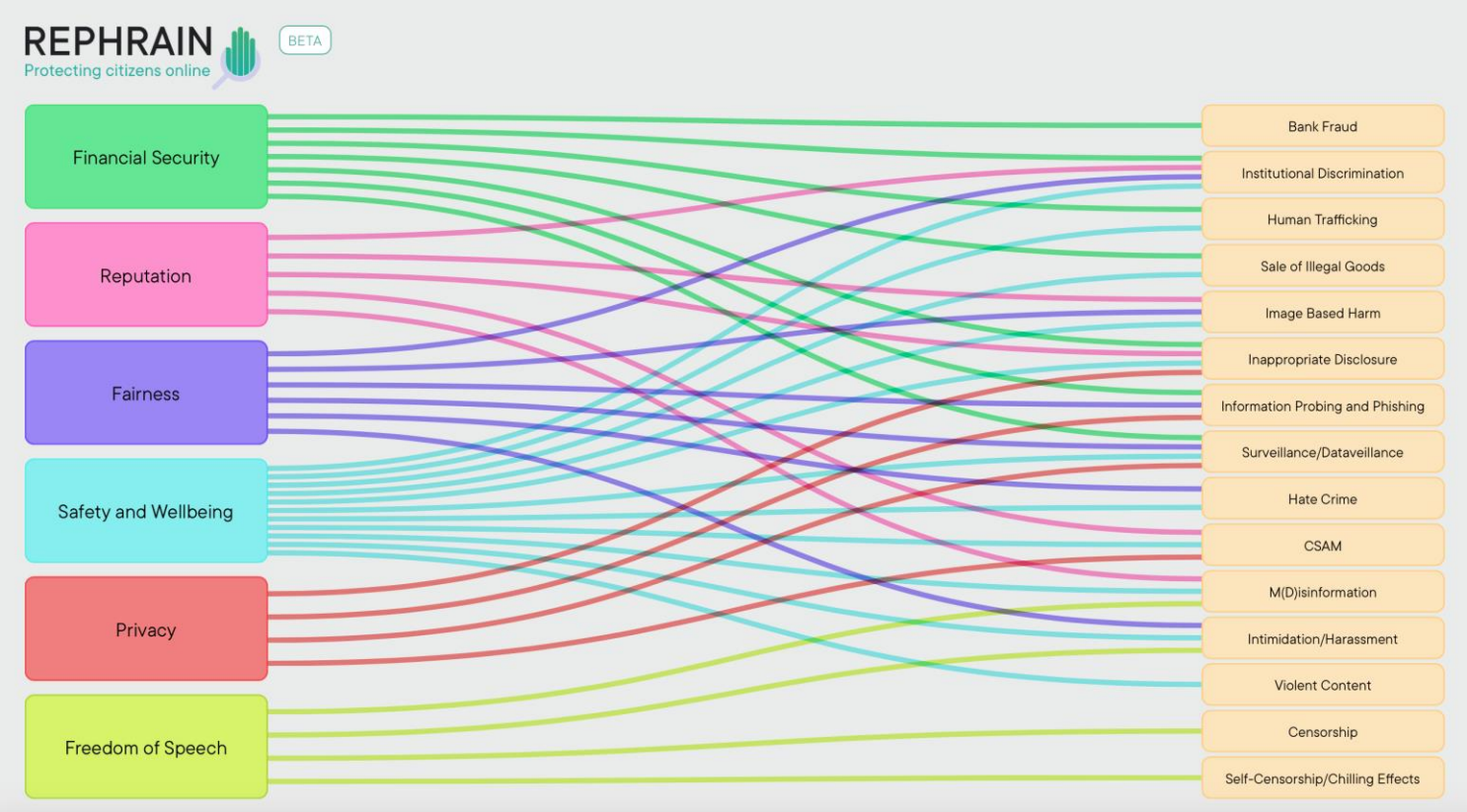
REPHRAIN Map

REPHRAIN Toolbox

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

REPHRAIN Map

REPHRAIN
Protecting citizens online

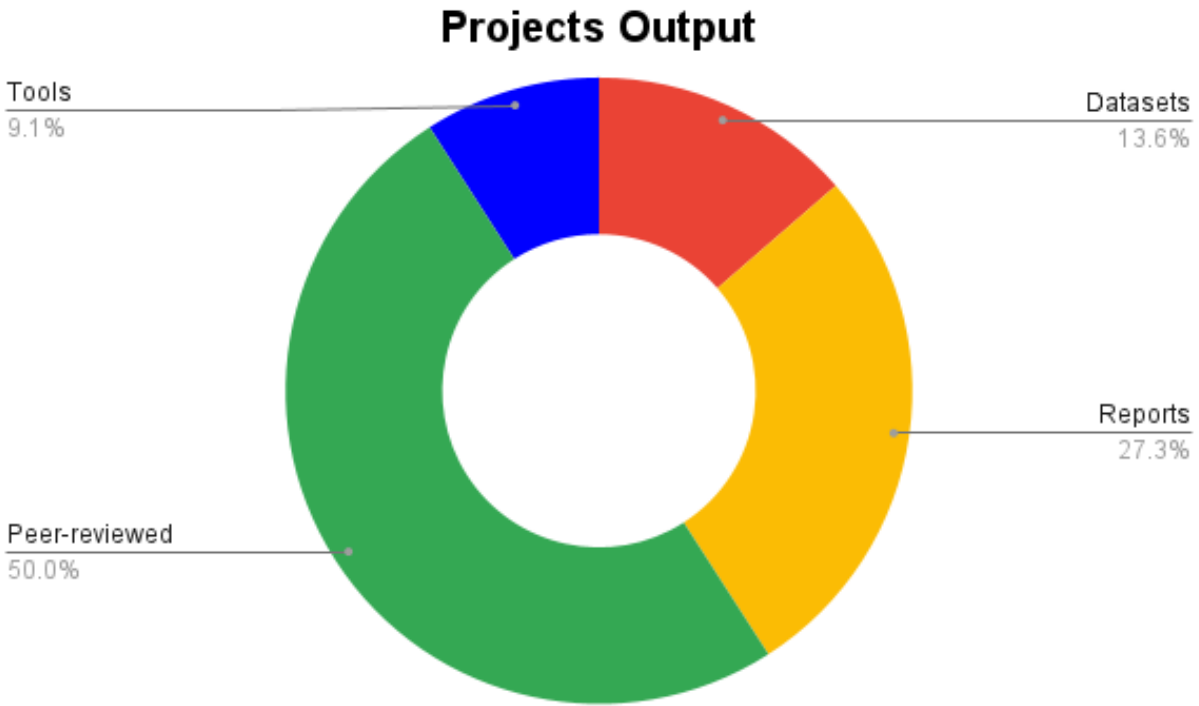


bris

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

REPHRAIN Toolbox

REPHRAIN
Protecting citizens online

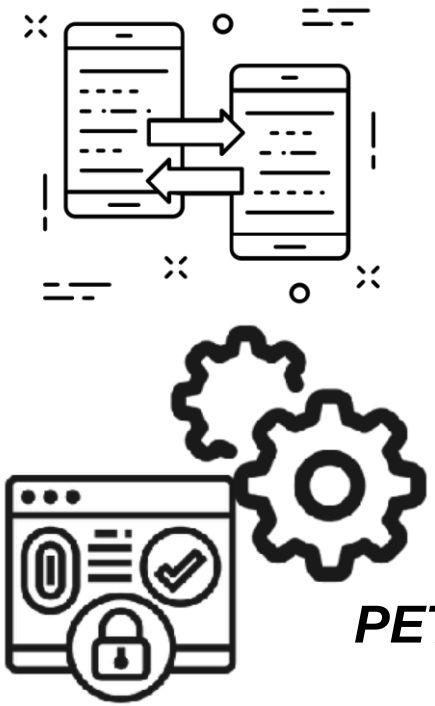


bristol.ac.uk

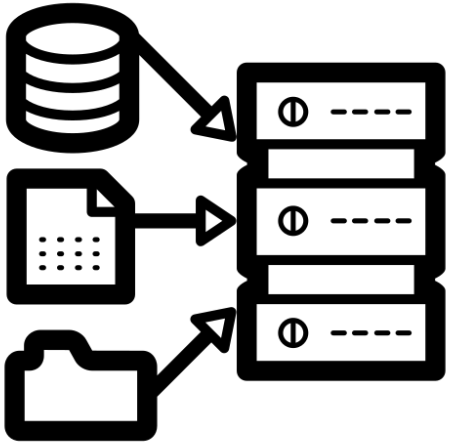
National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

Building Evidence Base

REPHRAIN
Protecting citizens online



PETS Testbed



REPHRAIN Data Archive

bristol.ac.uk

Sharing Best Practice

Best practices for data collection, as well as mechanisms for describing, checking, fixing and improving datasets; data storage; data sharing

Building rigorous research artefacts

Ethics review practices with a core ethos of protecting citizens online and responsible innovation

Safeguarding researchers and vulnerable users

Masterclasses on REPHRAIN research

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

Shaping Policy and Practice

REPHRAIN
Protecting citizens online

90 Engagement Activities

16 inputs into policy and regulatory initiatives

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

Shaping Policy and Practice

REPHRAIN
Protecting citizens online

Safety Tech Challenge Fund – Independent Evaluation

REPHRAIN invited by DCMS to provide an independent evaluation of Proof-of-Concept tools for preventing and detecting child sexual abuse media (CSAM) within end-to-end encryption (E2EE) environments within five different projects funded by the Safety Tech Challenge Fund.

The team is headed by ***Dr Claudia Peersman (University of Bristol)*** and joined by:

- Professor Corinne May-Chahal (Lancaster University)
- Professor Emiliano De Cristofaro (UCL)
- Dr Ryan McConville (University of Bristol)
- Dr Partha Das Chowdhury (University of Bristol)
- Dr Jose Tomas Llanos (UCL)

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

Shaping Policy and Practice

REPHRAIN
Protecting citizens online

DCMS App Security and Privacy Consultation Invited to and attended DCMS special invitation meeting to discuss	DCMS Connected tech: smart or sinister - call for evidence
Ofcom Online Harm consultation Follow up meeting with Ofcom to introduce REPHRAIN researchers with internal seminar to be given by Ofcom in November 2022	DCMS Misinformation and trusted voices inquiry
Home Office Unauthorised access consultation	UK Parliament (Science and Technology Select Committee) The Right to Privacy: Digital Data – call for evidence
UK Government Data: A New Direction consultation (joint response with CGLI)	

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

Shaping Policy and Practice

REPHRAIN
Protecting citizens online

Invited to attend the All-Party Parliamentary Group meeting on the Metaverse and Web 3.0.

Attended by Ola Michalec (REPHRAIN Policy and Regulation Strand) plus members of REPHRAIN looking at the online harms of VR and AR technologies.

Presented to over 60 people (including MPs and members of the House of Lords) and involved in in-depth discussion.

Shaping Policy and Practice

SoBigData – Research Infrastructure PPP

A 3-year ESFRI funded consortium to build on work undertaken as part of H2020 funding to create, implement and operate a research infrastructure.

Involves 31 partners from 13 European countries.

Project Preparation Phase (PPP) will focus on building:

- Legal and financial stability
- Sustainability
- Technical and governance maturity

Citizens at the Core

A paradigm shift from *Utility to Capability*

A *Manifesto* to empower users

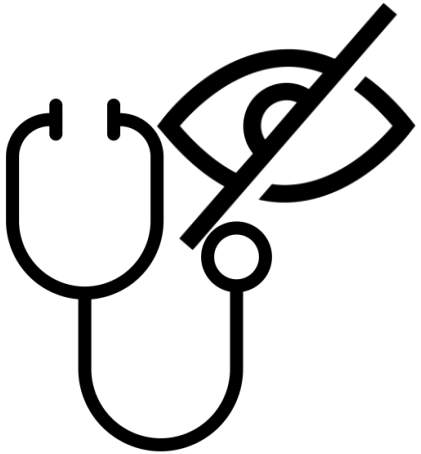
- Policy makers should assess deliberate influences to freedom
- Approaching capability through ethos
- Capability approach to assess the circumstances of the marginalised and non-participants
- Democratic participation to evolve a list of basic minimum online protections
- A reasoned understanding of winners and losers
- Individuals should value participating in the online community

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

Citizens at the Core

REPHRAIN
Protecting citizens online

Supporting vulnerable user groups



Privacy Clinics

Tackling violence against women and girls online

bristol.ac.uk

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

Citizens at the Core

REPHRAIN
Protecting citizens online

REPHRAIN Sandpit

Transforming REPHRAIN research into actionable impacts for protecting citizens online

bristol.ac.uk

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

And finally

REPHRAIN
Protecting citizens online

Proceedings on Privacy Enhancing Technologies Symposium

PoPETs | Go to PETS

Home | CFPs ↓ | Authors ↓ | Reviews ↓ | Proceedings | Awards ↓ | Sponsorship | Code of conduct

To be hosted by REPHRAIN in July 2024 at University of Bristol

bristol.ac.uk