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

Strategic Funding Call 1 – 19 April 2021

Closing date: 21 May 2021

REPHRAIN (Privacy, Harm Reduction and Adversarial Influence Online Research Centre) is an EPSRC funded research centre that forms part of the wider UKRI investment focusing on protecting citizens online. REPHRAIN explores how to keep people safe online while allowing them to fully participate in digital technologies and the contributions they make to innovative, inclusive and healthy economy and society.

REPHRAIN involves researchers in Computer Science, International Relations, Law, Psychology, Management, Design, Digital Humanities, Public Policy, Political Science, Criminology and Sociology. It will build and lead the UK's world-leading interdisciplinary community on protecting citizens online and provide a clear single front door to engage and build capacity with government, industry and citizens.

REPHRAIN was launched in October 2020 with funding from the EPSRC and is a consortium of five academic institutions: the University of Bristol, University of Bath, University of Edinburgh, University College London and King's College London. Further details can be found here https://www.rephrain.ac.uk/.

Call details

Since its launch, the Centre team has been engaging in a series of scoping activities – involving consultation workshops as well as literature reviews with the aim of identifying priority areas for the first REPHRAIN Strategic Funding Call.

The total funding for this call is £500,000 (at 100% fEC), of which 80% will be funded by REPHRAIN. We expect to fund multiple proposals from this fund and will consider larger proposals that address more than one topic area. All funded projects must be completed, with all deliverables, by **30 June 2022**. Proposals should be submitted by **4pm on 21 May 2021** at https://easychair.org/conferences/?conf=rephrainsfc1. The Strategic Funding decision panel will meet **w/c 21 June 2021** and decisions will be communicated **w/c 28 June 2021**.

Call topics

This strategic funding call is for projects that relate to REPHRAIN's missions and research challenges. We particularly encourage proposals that focus on the following themes that have emerged from the scoping work undertaken:

- **Testbeds for detecting, disrupting and investigating online harm.**
  Existing evidence suggest that testing of the effectiveness of systems is largely based on formal proofs and assumptions [3]. However, this may limit the general understanding about how systems will perform in real world scenarios. Regarding online harms, there is a need for testbeds for adequate testing and refining against real world conditions [14]. A technical challenge is around testing tools that deal with category of harms that involve sensitive content. Therefore, there is a need for development of testbeds for studying the effectiveness of harm mitigation approaches under realistic conditions. REPHRAIN is already developing a PETS testbed as part of this programme. We welcome proposals for additional testbeds on online harms to be developed and integrated into the REPHRAIN testbed.

- **Novel awareness mechanisms.**
  Research is needed on new ways of raising citizens' awareness about various threats in a manner that they are not overloaded with information. One related challenge is creating spaces to stimulate conversation and awareness about privacy and online harm across different generational groups. Adoption of technical tools and protection mechanisms are often dependent on the various levels of threat understanding. They also assume users are technically proficient and are always updating their mental models. There is a need for new ways of raising awareness (e.g., safety and privacy statutory labelling metrics [4, 9]) especially for vulnerable groups such older citizens and children without exposing them to further threats and harms. Research should also provide new types of online (and offline) spaces that enable such conversations.

- **Negotiation and conflict resolution mechanisms.**
  In social networks and cloud computing systems, existing mechanisms allow users to "unfriend" or "change permissions" to resolve issues. However, such actions may lead to power imbalance where some users are denied accessed to co-owned items. It is also challenging to balance the need to honour users' decision to change their preferences but still give others access to co-owned items. In shared devices such as smart speakers and cameras, it is challenging to manage and honour users' changing privacy preferences. Existing efforts usually oversimplify [15] the conflict resolution process which sometimes leads to mismatch between actual behaviour and the proposed mechanisms. They also lack appropriate practical evaluations of their acceptance in real-world applications. There is a need for new ways which recognise the complexity of user behaviour and tools to enable effective conflict resolution and collaboration between users. New socio-technical approaches are needed to provide negotiated privacy in shared online settings while mitigating the impact on access or service to co-owned items or shared devices.

- **Establishing scalable trust.**
  A persistent issue for systems engineering is that of trust. It is difficult for users to gather and understand information about remote entities and their underlying processes, sources, and privacy policies. Despite this, users trust automated systems and online platforms on a daily basis to access a range of services as well as information. While automation has many benefits in terms of efficiency and accuracy, a growing body of research suggests that automation may exacerbate existing inequalities and lead to discrimination, bias and exclusion [7]. Recent studies show that algorithmic bias is not solved by merely making them agnostic to certain parameters such as ethnicity or gender [6]. Moreover, while social network platforms are significantly used for spreading information, opinions and ideas, they pose significant challenges to trust in information as they can also be used to propagate fake news, pseudo-scientific knowledge, misinformation and hate speech. Good quality, safe and trustworthy systems and sources of information are critical for participating online. Yet this is a complex and highly politicised issue. When it comes to trust in information, solutions cannot be reduced to just detecting, fact-checking and taking down content as often there are not clear cut lines between what constitutes good-faith information, opinions, fake news, disinformation, and incomplete or misleading information [10, 1]. Consequently, there is a need for mechanisms that improve people's trust in algorithmic systems, online platforms, and the information they help to disseminate without creating overload to users. These may involve trustworthy oversight mechanisms, algorithmic fairness and accountability.

- **Data minimisation and deletion in online platforms.**
  Dependency on online systems to share and store data has grown immensely over the last few years. However, collecting, storing or sharing user data poses various threats to their privacy. Two possible ways of reducing the impact of a possible privacy breach are not collecting certain data (i.e., data minimisation [2]) or completely deleting data that is no longer needed (i.e., assured deletion [11, 13]). However, these solutions pose two fundamental challenges: (1) collecting and using less data without compromising the benefits of its use or the service, and (2) providing assured data deletion. The advent of smart home devices, complex cloud infrastructures, Machine Learning techniques, and ubiquitous technologies all make it challenging to collect less data or to completely delete data when it is no longer needed [11, 13]. Moreover, with regards to data deletion, prior works [12, 8, 5] suggest that users have challenges in understanding and completing data deletion. Research should, therefore, explore novel ways in which less data could be collected and used but still yielding maximum benefits. In addition, research should also develop tools and approaches to ensure complete data deletion from various technologies and devices. These efforts should include making minimisation and deletion usable and understandable to citizens.

The above are indicative topics and we welcome proposal on additional related topics.

Funding

The total amount available for this Call will be up to £500,000 at 100% full Economic Cost (fEC), of which 80% fEC (i.e., up to £400,000) will be made available to successful applicants. In practical terms this means that UK HEI researchers should cost their projects using the same process as they would cost a UKRI grant. All costs should be inclusive of VAT and/or any other applicable tax. The duration of work proposed under this Call should not last more than 12 months and should run between **01 July 2021** and **30 June 2022**. REPHRAIN will not reimburse costs associated with the development or submission of a proposal.

Proposals should be costed and approved by the applicant's organisation before submission.

Submission

Please submit the proposal as a single PDF by **4pm on the 21 May 2021** using the form and upload system at: https://easychair.org/conferences/?conf=rephrainsfc1. If you do not already have an EasyChair account you will need to set one up here. If you already have an account, you should be able to access the REPHRAIN SFC 1 submission page using your current credentials. Please ensure you select the role of author before submitting your proposal.

Submissions should not exceed five pages plus short CVs, comprising:

1) The research challenge to be addressed and its alignment with REPHRAIN's missions and RIEI (Responsible Inclusive Ethical Innovation) approach (1 page max)
2) Interdisciplinarity objectives (1/2 page max)
3) Proposed methodology (1 ½ page max)
4) Proposed outcomes (deliverables with timescales) and potential for integration with the REPHRAIN toolbox (1 page max)
5) Financial summary (divided into directly incurred and allocated staff costs, travel, subsistence and other costs, estates and indirect costs. (1 page max). The costs should be in sufficient detail to allow for value for money judgements to be made.

Please attach short (2 page) CVs for all applicants and named researchers at the end of the proposal. Please ensure the proposal and CVs are merged as one single PDF. A submission template can be found on the REPHRAIN website.

All documents must be completed in single-spaced typescript in Arial pt 11 or other sans serif typeface of equivalent size, with margins of at least 2cm. Arial narrow and Calibri are not allowable font types and page limits must not be exceeded. Each section listed above (1-5) should be clearly labelled.

Eligibility

The Call is open to Higher Education Institutions who can demonstrate a capability to deliver a high-quality programme of research. We strongly encourage applications from researchers in all disciplines and encourage proposals that are interdisciplinary and involve strong engagement and partnerships with non-academic stakeholders. This call will follow the standard EPSRC eligibility criteria.

Assessment

All proposals will be reviewed by at least two expert peer reviewers, and then evaluated by a Strategic Fund decision panel. Applications that are not submitted in the format requested in above, or that are outside of the scope of this call, may be rejected without recourse to peer review.

Criteria

Submissions will be scored by peer reviews across the following domains:

1) Understanding of the challenge and its national importance
2) Quality and rigour of methodology
3) Responsible innovation
4) Potential impact and integration with the REPHRAIN toolbox
5) Value for money and deliverability
6) Team track record, particularly interdisciplinarity of team

Grant conditions

Successful applicants will receive an offer letter that will outline the terms of the sub-contract with REPHRAIN. These are standard UKRI terms and conditions, but with some minor amendments related to the source of funding and relationship with the REPHRAIN research centre. **Applicants should make sure that these terms are acceptable to their organisation before applying for funding. The terms are not negotiable. Copies of the contract are available here.**

Equality, Diversity and Inclusion

The long-term strength of the UK research base depends on harnessing all the available talent and the Research Councils together developed the ambitious UKRI Equality, Diversity and Inclusion Action Plan. In line with the UKRI's policies on equality, diversity and inclusion, we expect that equality, diversity, and inclusion are embedded at all levels and in all aspects of applicants' research proposals.

We are committed to supporting the research community in the diverse ways a research career can be built. Therefore, we welcome applications from researchers who job share, have a part-time contract, need flexible working arrangements or those currently committed to other longer, large existing grants.

References

[1] Melanie Freeze, Mary Baumgartner, Peter Bruno, Jacob R. Gunderson, Joshua Olin, Morgan Quinn Ross, and Justine Szafran. Fake Claims of Fake News: Political Misinformation, Warnings, And The Tainted Truth Effect. Political Behavior.

[2] Seda Gürses, Carmela Troncoso, and Claudia Diaz. Engineering Privacy by Design Reloaded. In Amsterdam Privacy Conference, pages 1–21, 2015.

[3] C. Herley and P. C. Van Oorschot. SoK: Science, Security and the Elusive Goal of Security As A Scientific Pursuit. In 2017 IEEE Symposium on Security and Privacy (SP), pages 99–120, 2017.

[4] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach. In Elizabeth D. Mynatt, Don Schoner, Geraldine Fitzpatrick, Scott E. Hudson, W. Keith Edwards, and Tom Rodden, editors, Proceedings of the 28th International Conference on Human Factors in Computing Systems, CHI 2010, Atlanta, Georgia, USA, April 10-15, 2010, pages 1573– 1582. ACM, 2010.

[5] Mohammad Taha Khan, Maria Hyun, Chris Kanich, and Blase Ur. Forgotten But Not Gone: Identifying the Need for Longitudinal Data management in cloud storage. In Regan L. Mandryk, Mark Hancock, Mark Perry, and Anna L. Cox, editors, Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, CHI 2018, Montreal, QC, Canada, April 21-26, 2018, page 543. ACM, 2018.

[6] Jon Kleinberg, Jens Ludwig, Sendhil Mullainathan, and Ashesh Rambachan. Algorithmic Fairness. AEA Papers and Proceedings, 108:22–27, May 2018.

[7] Jon Kleinberg, Jens Ludwig, Sendhil Mullainathan, and Cass R Sunstein. Discrimination In The Age of Algorithms. Journal of Legal Analysis, 10:113–174, 04 2019.

[8] Ambar Murillo, Andreas Kramm, Sebastian Schnorf, and Alexander De Luca. “If I press delete, it’s gone” - User Understanding of Online Data Deletion and Expiration. In Mary Ellen Zurko and Heather Richter Lipford, editors, Fourteenth Symposium on Usable Privacy and Security, SOUPS 2018, Baltimore, MD, USA, August 12-14, 2018, pages 329–339. USENIX Association, 2018.

[9] Pardis Emami Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. Ask The Experts: What Should Be on an IoT Privacy and Security Label? In 2020 IEEE Symposium on Security and Privacy, SP 2020, San Francisco, CA, USA, May 18-21, 2020, pages 447–464. IEEE, 2020.

[10] Jason Pielemeier. Disentangling Disinformation: What Makes Regulating Disinformation so Difficult? Symposium: News, Disinformation, and Social Media Responsibility. Utah Law Review, 2020(4):917–940.

[11] Kopo M. Ramokapane, Awais Rashid, and Jose M. Such. Assured Deletion in the Cloud: Requirements, Challenges and Future Directions. In Edgar R. Weippl, Stefan Katzenbeisser, Mathias Payer, Stefan Mangard, Elli Androulaki, and Michael K. Reiter, editors, Proceedings of the 2016 ACM on Cloud Computing Security Workshop, CCSW 2016, Vienna, Austria, October 28, 2016, pages 97–108. ACM, 2016.

[12] Kopo M. Ramokapane, Awais Rashid, and Jose M. Such. ”I feel stupid I can’t delete...”: A Study of Users’ Cloud Deletion Practices and Coping Strategies. In Thirteenth Symposium on Usable Privacy and Security, SOUPS 2017, Santa Clara, CA, USA, July 12-14, 2017, pages 241–256. USENIX Association, 2017.

[13] Joel Reardon, David A. Basin, and Srdjan Capkun. SoK: Secure Data Deletion. In 2013 IEEE Symposium on Security and Privacy, SP 2013, Berkeley, CA, USA, May 19-22, 2013, pages 301–315. IEEE Computer Society, 2013.

[14] Ali Tekeoglu and Ali Saman Tosun. A Testbed for Security and Privacy Analysis of IoT devices. In 13th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2016, Brasılia, Brazil, October 10-13, 2016, pages 343–348. IEEE Computer Society, 2016.

[15] Kurt Thomas, Chris Grier, and David M. Nicol. unFriendly: Multi-party Privacy Risks in Social Networks. In Mikhail J. Atallah and Nicholas J. Hopper, editors, Privacy Enhancing Technologies, 10th International Symposium, PETS 2010, Berlin, Germany, July 21-23, 2010. Proceedings, volume 6205 of Lecture Notes in Computer Science, pages 236–252. Springer, 2010.