Trust, Identity, Privacy and Security in the Digital Economy

Call type: Invitation for Proposal

Closing date: 16:00 on Tuesday 13 October 2015

Related Themes: Digital Economy; ICT; Global uncertanties

If you are planning to apply, please complete a compulsory "Intent to Submit" form by Monday 14 September 2015.

Summary

The Research Councils UK Digital Economy Theme and the cybersecurity strand of the Partnership for Conflict, Crime and Security are investing up to £10 million to support user-driven and interdisciplinary research that solves real problems in establishing trust, identity, privacy and security in the digital economy.

Funding is available to support projects that demonstrate

(1) That the research challenge has been co-created with user(s) and across disciplines;

(2) That the research will be conducted "in the wild" exposing the research to potential users and beneficiaries;

(3) How the potential impact of the research will be realised by user(s) and/or related beneficiaries.

The call aims to enable researchers to expose and test potentially transformative, interdisciplinary research ideas with beneficiaries – for example, businesses, government, third sector and/or citizens – in order to get closer to achieving viable and scalable propositions for deployment. The call intends to attract participants collaborating across the full range of social sciences, arts and humanities, and engineering and physical sciences. We strongly encourage potential applicants to collaborate in identifying and submitting proposals where to do so would improve the quality of the research and that present a real opportunity for the UK to become internationally leading.

The application process will take the form of "Intent to Submit" and full proposals, which will be assessed by postal peer review and prioritisation panel. You must complete an "Intent to Submit" form by **14 September 2015**; applicants who do not do this will be ineligible for the call. We will make PI name, institution and title of the "Intents to Submit" publically available on the call website to facilitate collaboration building. You will not be held to these details in the full proposal.The closing time and date for full proposals is **16:00 on 13 October 2015**.

Background

In June 2014, the Research Councils UK Digital Economy Theme held a workshop to capture “bottom-up” research challenges from a broad cross section of the academic and user communities addressing the question "What is going to be the main societal, economic or cultural challenge associated with the digital economy space over the next five to ten years?"[1]. One tangible outcome of this workshop was to inform the development of a new research priority area for the RCUK Digital Economy Theme in Trust, Identity, Privacy and Security for which we are making research funding available via fellowships[2] as well as this targeted funding call.

Trust, identity, privacy and security
The potential exists for personal data, regarding for example behaviour, lifestyles and consumption, to transform business models and underpin new public and private services in the digital economy. Simultaneously, the emerging application opportunities offered to individuals by new technologies, such as the Internet of Things, across healthcare, sustainable living and quality of life, rely increasingly on the capture and processing of personal data.

A key element to enabling the transformational potential of personal data is an ecosystem that protects the interests of the individual and builds confidence that digital economy services will use personal information responsibly while enabling new commercial and societal opportunities for innovation. To enable technical innovations in this space that can scale to deliver meaningful economic and social impact and secure competitive advantage for the UK requires interdisciplinary and user-driven research. Research into solutions to these challenges will need to be co-created with individuals, communities, government, businesses and the 3rd sector.

Focus of Call

The aim of this call is to support co-created, user-driven and interdisciplinary research that addresses real problems in the broad areas of trust, identity, privacy and security in the digital economy. We want to support collaborations that move research out of the lab into demonstrable use cases for scalable deployment, exposing the research to potential beneficiaries. Your research projects should be interdisciplinary and user-driven and should blend and balance the technological, economic, cultural, social, behavioural and political challenges around trust, identity, privacy and security and incorporate legal, regulatory and international aspects where appropriate. It is expected that there will be engagement with business, policy makers, users and/or the third sector and these activities are encouraged in this call. **We strongly encourage potential applicants to collaborate in identifying and submitting proposals where to do so would improve the quality of the research** and present a real opportunity for the UK to become internationally leading.

[1] http://www.well-sorted.org/explore/DESM2014/documents/DESMDocRelease1.0.pdf
[2] https://www.epsrc.ac.uk/skills/fellows/areas/priorityareas/digitaleconomy/

A) Research Themes

We wish to fund projects that are each seeking to address one or more of the following research themes. You must have a clear statement of the novelty of the research and the research questions to be addressed as well as their relevance to the research themes below. You must articulate a coherent and ambitious vision for the project. We are interested in encouraging breadth of perspective and a diversity of research approaches. We intend a broad interpretation of each research theme and there may be topics that underpin these themes; no specific areas are excluded.

i. Systems and their Ecosystems

Transparency of data processing and better access to the algorithms operating on personal data may by itself be of little direct benefit to most users as the processes described are too complex. The emerging discipline of Human Data Interaction (HDI)[3] places the human at the centre of these data and seeks to understand how systems design can provide comprehensible mechanisms for users and citizens to understand, influence and benefit from the data and their use.

Research challenges include:

- Developing mechanisms to improve data quality and data processing algorithms, and to give people control over lifetime, scope and visibility of their personal data;
- Co-creating HDI approaches with technologies to provide desirable outcomes using shared personal data to offer insight and information both to individuals and society, while respecting privacy;
- Understanding the agency, behaviour and rights of consumers and citizens (taking into account demographic, cultural, economic factors etc.) who, while clearly expressing a desire for privacy, make daily compromises to use services they feel (socially) essential. How should regulatory and legal frameworks reflect/adapt these tensions and how will companies/organisations respond?

ii. Privacy Preserving Design and Anonymisation

Differential privacy, “small data” processing and various probabilistic techniques have all been investigated as privacy preserving technologies; continued research on such techniques and their interfaces is essential for increasing the arsenal for privacy by design. At the same time, many of these techniques may be prone to re-identification through data linkage.

Research challenges include:

- Fundamental research challenges on how data can be obfuscated such that re-identification is difficult, whether by being computationally unattractive, resulting in only aggregate information, or otherwise;
- The development of interoperable and scalable privacy-preserving techniques that maximise synergies between privacy and security and emerging new business models and markets;
- Understanding the ethical issues of informed consent (knowing what you are disclosing and for what purpose), information creep (use of

[3] http://hdiresearch.org/

information given for one purpose to satisfy another purpose), and data control (whose data are they anyway).

iii. Trusting and Consenting to Pervasive and Ubiquitous Computing

Internet of Things sensors will likely be pervasive and ubiquitous in future cities and homes. In this environment there are fundamental questions as to whether there can be "informed consent" in the use of personal data. There is a danger that systems are legitimised solely by the "legitimate interests" of the data collector, which may not play out well with citizens in creating trust (e.g. Bluetooth bins).

Research challenges include:

- How can "Smart" environments be constructed so as to be comprehensible and feel safe for users;
- What are the underlying contexts and competing attitudes of the data collector? Design is also key in terms of building trust into systems from the beginning;
- How is trust in cyber infrastructure, and the resultant economic activity, affected by demographic, ethnographic, cultural and experimental factors and their influence on users' behaviour and perceptions with respect to smart interventions and related issues.

iv. Identity and Identity Mechanisms

There are concerns that current online identity mechanisms, whether commercial or governmental, are another effective way to track activity. These identity mechanisms may reduce the ability to adopt multiple legitimate identities for example within versus outside the family.

Research challenges include:

- Understanding the landscape and value of identity policies adopted by organisations and their impacts and effectiveness (e.g. the effectiveness of "real name policies" in reducing antisocial behaviour);
- Investigating what mechanisms for digital identity can support a rich digital society, for example based on distributed consensus protocols like blockchain[4,5];
- A holistic understanding of the technological, economic, cultural, social, behavioural and political challenges of how trust and identity (among individuals and groups) is developed, maintained, transformed and lost in the digital world building on previous work[6].

v. Cybersecurity and its Economics and Human Dimensions

---

[4] http://www.nemode.ac.uk/wp-content/uploads/2015/02/2015-Bit-Coin-risk-analysis.pdf

[5] http://www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf

[6] For example, the work of the EMoTICON (http://www.esrc.ac.uk/news-and-events/press-releases/31370/empathy-and-trust-in-communicating-online.aspx), Digital Personhood (http://www.digitalpersonhood.org/index.php), "Who do you think you are?" (http://gow.epsrc.ac.uk/NGBOViewGrant.aspx?GrantRef=EP/J005266/1) and Identity Network communities (http://gow.epsrc.ac.uk/NGBOViewGrant.aspx?GrantRef=EP/K00333X/1).

- With the increasing scale and complexity of cyber threats, we must simultaneously investigate the ecosystem, the economics and the software engineering approaches that can support and foster more advanced cybersecurity thinking and approaches in the commercial sector. What are the opportunities for risk-based approaches?

Research challenges include:

- Understanding how much individuals and organisations are able and willing to invest in return for cybersecurity;
- Understanding the value of what is being secured by the provider, and the value of what is being requested of the individual. A full understanding of these issues will support the development of cybersecurity practice that are endorsed from their conception by active citizens as end-users and would significantly improve the resilience of our systems;
- Finding new ways to protect individuals and organisations from the increasing scale and complexity (across multiple digitally-connected supply chains) of cyber threats and the dangers of single points of failure with increasingly centralised cloud computing, especially for core infrastructure.

vi. Broad Applications of Distributed Ledger Technologies

Distributed ledger technologies refers to a set of technologies that make possible the secure transfer of ownership of anything of value over the internet, with a permanent and transparent record of what has taken place without the need for a trusted third party. This could have applications in many contexts including retail payment services, transfer of financial instruments, land registry, health data or other (digital and physical) assets as well as in cybersecurity and digital civics and myriad unimagined domains. Such applications could reshape our concepts of how our economy operates, is measured and controlled making possible a vision of a 'smart' economy that can support diverse scenarios of monetary and non-monetary value exchange between individuals and organisations and in the future, "smart" machines and "smart" entities. However the speed of technological advancement in this area has outpaced the required changes in societal, ethical, legal and business frameworks limiting confidence in, trust and adoption of these systems by individuals, communities, organisations and states.

Research challenges include:

- Developing scalable and resilient distributed ledger technologies coupled with appropriate balance across permissions and privacy versus transparency and accessibility and potentially offering opportunity for recourse or withdrawal from the "blockchain";
- Understanding the requirements needed to encourage and secure the trust of individuals, communities and organisations in the use of distributed ledger systems for important applications e.g. voting, distribution of welfare, insurance etc and the justifiable benefits brought about by their use for these purposes.
- Development of socially oriented distributed ledger technology – identifying uses of distributed ledger that deliver social benefit e.g. distributing aid and public services;

B) Interdisciplinary Research Co-created with Users

Projects should be co-created with users and across disciplines and you must describe:

- The specific context or real world scenario being addressed. You may wish to demonstrate this in your proposal using a design fiction or storyboard approach;
- The research challenge(s) being addressed, including how the research has been co-created with the end-user(s) and across relevant key disciplines;
- How potential beneficiaries will be exposed to the research and potential impacts e.g. via demonstrable use cases for scalable deployment;
- Potential risks associated with the project and options to mitigate this risk;

Activities could cover the testing of new technologies and methods with potential beneficiaries or in the user(s) domain or looking at new ways of using existing technologies/methods. Applications should not aim to develop a technology or methodology purely of commercial benefit to an individual company.

Examples of the types of research being sought can be found at the following panel meeting links:

- **http://gow.epsrc.ac.uk/NGBOViewPanelROL.aspx?PanelId=1-3B4R1&RankingListId=1-3B4R8**
- **http://gow.epsrc.ac.uk/NGBOViewPanelROL.aspx?PanelId=1-WKXII&RankingListId=1-WKXIN**
- **http://gow.epsrc.ac.uk/NGBOViewPanelROL.aspx?PanelId=1-1F64MT&RankingListId=1-1F64TV**

For more information about EPSRC's portfolio and strategies, see our website: https://www.epsrc.ac.uk/research/ourportfolio/

C) Brokerage Event

We are hosting a brokerage event in partnership with the Personal Data and Trust Network[7] on **03 September 2015** at the Digital Catapult Centre for you to find potential collaborators and/or to test your ideas for this call. **Attendance is optional.** We are offering the opportunity for applicant groups who cannot attend the brokerage event to submit their details, which we will make publically available to attendees (both academics and users) on the day. Please submit your details via the registration[8] webpage below. The feedback you receive from the brokerage event will not form any part of the assessment process for your proposal. **Further details are available on the registration page[8].**

D) Networking

We recognise that many of the research challenges will require establishing global standards and 'principles' across institutions and sectors that is beyond

[7] The Personal Data and Trust Network is a partnership across the Digital Catapult, the Knowledge Transfer Network and the EPSRC that brings together industry, the public sector and researchers to support the UK in becoming the global leader in trust and responsible innovation with personal data. http://www.pdtn.org

[8] https://www.eventbrite.co.uk/e/brokerage-event-trust-identity-privacy-and-security-funding-call-registration-18002057639

the scope of any one researcher, business or community. Thus, we expect you to ring fence **up to 5% (of the total FEC proposal value) of your funds to support networking activities** across the successfully funded bids and with users via the Personal Data and Trust Network and other relevant networks[9] in order to help co-create and disseminate the outputs and outcomes of your research. There is no pre-determined composition of the costs for networking activities. It is for you to determine the best use of these funds and deem what is most appropriate for the research programme. The costing and use of these networking funds must be clearly identified in the Pathways to Impact statement in your full proposal.

Successful applicants will also have access to the Digital Catapult's Trust Framework Initiative[10] that aims to create a standardised set of consumer-centric guidelines for organisations to follow to establish a trustworthy and interoperable personal data ecosystem linking citizens, government and the private sector.

E) Societal Implications and Ethical Issues

We recognise that some areas of the Digital Economy have the potential to raise societal, ethical, philosophical, legal and regulatory issues and risks. Consideration of these issues is essential to ensure that the research carried out is considered within a societal context and that any such issues that are raised are fully explored as the research develops. For further information on ethical requirements applicants are referred to the following guidance documents:

http://www.esrc.ac.uk/about-esrc/information/framework-for-research-ethics/index.aspx
http://www.mrc.ac.uk/research/research-policy-ethics/

Funding available

Up to £10 million has been earmarked for this call that includes up to £3 million of possible case by case funding from the cybersecurity strand of the Partnership for Conflict Crime and Security. Subject to the quality of the submissions received, it is anticipated that we will fund up to 10 proposals.

Equipment

Where possible, researchers are asked to make use of existing facilities and equipment, including those hosted at other universities. If equipment is needed as part of the research proposal, applicants must follow EPSRC's rules for requesting equipment over £10,000 in value. Individual items of equipment up to the current OJEC (Official Journal of the European Communities) procurement threshold can be included on research proposals submitted through this call, but research organisations will be expected to make a contribution to the cost. All requests for single items of equipment above the current OJEC threshold will need to go through a separate process which will assess the strategic need for the equipment and how to ensure maximum usage. These proposals will be assessed through the separate Strategic Equipment peer review process. For more information on equipment funding, please see:

[9] Such as the EMoTICON, Digital Personhood, WDYTYA and Identity research communities
[10] http://www.digitalcatapultcentre.org.uk/open-calls/trust-framework-initiative

http://www.epsrc.ac.uk/research/ourportfolio/themes/researchinfrastructure/subthemes/equipment/.

The current OJEC threshold can be found at:
http://www.epsrc.ac.uk/research/facilities/equipment/

Eligibility

For information on the eligibility of organisations and individuals to receive EPSRC funding, see the EPSRC Funding Guide:
https://www.epsrc.ac.uk/funding/howtoapply/fundingguide/

As this call is a targeted funding opportunity provided by EPSRC, higher education institutions, and some research council institutes and independent research organisations are eligible to apply. A list of eligible organisations to apply to EPSRC is provided at: http://www.rcuk.ac.uk/funding/eligibilityforrcs/

How to apply

Intent to Submit form

To be eligible for this call you must complete an "Intent to Submit" form available on the call webpage by the **14 September 2015**. Applicants who have not completed this form will be ineligible for the call. Please note that to facilitate collaboration building **we will be making the following information – Principal Investigator name; Institution; Project title; Desired collaborators – in your "Intent to Submit" form publically available on the call website during the week commencing 14 September 2015.** The information that you provide in your "Intent to Submit" form will not be used in the assessment process.

Submitting full proposal application

You should prepare and submit your full proposal using the Research Councils' Joint electronic Submission (Je-S) System (https://je-s.rcuk.ac.uk/).
When adding a new proposal, you should select:

- Council 'EPSRC'
- Document type 'Standard Proposal'
- Scheme 'Standard'
- On the Project Details page you should select the [Trust, Identity, Privacy & Security in the Digital Economy (DE TIPS)] call.

Note that clicking 'submit document' on your proposal form in Je-S initially submits the proposal to your host organisation's administration, not to EPSRC. Please allow sufficient time for your organisation's submission process between submitting your proposal to them and the call closing date. We must receive your application by **16:00 on 13 October 2015**.

Guidance on the types of support that may be sought and advice on the completion of the research proposal forms are given on the EPSRC website (https://www.epsrc.ac.uk/funding/howtoapply/preparing/) which should be consulted when preparing all proposals.

Guidance

Guidance on writing application

As well as the Je-S form, the following documents should be submitted:

- Case for support: should be up to 8 pages in total, to include:
    - Two-page track record, which should detail the relevant expertise that each investigator will bring to the research
    - Six-page description of the proposed research focus and people-based activity streams. This should include a clear statement of the proposal's vision, and how each strand of activity complements this vision.
- Pathways to Impact: should be up to two pages and is primarily for detailing the activities which will help develop potential economic and societal impacts. Please detail how the proposed research project will be managed to engage beneficiaries and increase the likelihood of impacts. More information on preparing the impact plan and on impact can be found on the EPSRC website at:
  https://www.epsrc.ac.uk/funding/howtoapply/preparing/impactguidance/
  https://www.epsrc.ac.uk/funding/howtoapply/preparing/writing/resourcesimpact/
  https://www.epsrc.ac.uk/innovation/publicengagement/innovativeexamplesofpathwaystoimpact/
- Justification of resources: should be up to two pages. This should be a narrative description of the need for the resources requested.
- Work plan: should be up one page. It is not expected that this will be a Gantt chart for the whole time of the project, but should include a comprehensive plan for the start of the project and then refer to the management strategy to give appropriate milestones for when important decisions on the direction of the research will be taken.

For advice on writing proposals see:

https://www.epsrc.ac.uk/funding/howtoapply/preparing/

User Engagement Strategy

You are required to develop and execute a strategy for engaging with potential users of the research funded in the project. Resources for this activity are to be requested as part of the Pathways to Impact and must be justified in the application. This strategy should be reviewed and updated regularly as part of the formal management of the grant.

The strategy should cover:

- How and when potential users have been / will be identified;
- What form the engagement will take;
- What steps will be taken to ensure that outputs of the research are made available to potential users, and

- Suitable metrics for determining the success of the strategy in delivering value to users.

Responsible Innovation

Scientific research has the ability to not only produce understanding, knowledge and value, but also unintended impacts, questions, ethical dilemmas and, at times, unexpected transformations in social life. We recognise that we have a duty of care to promote approaches to "responsible innovation" which will initiate on-going reflection about the potential ethical and societal implications of the research that we sponsor on behalf of the taxpayer and to encourage our research community to do likewise. As a research sponsor, our aim is to build capacity within our research community to discuss and consider social and ethical questions. Therefore we expect applicants to adhere to the Framework for Responsible Innovation (http://www.epsrc.ac.uk/research/framework/). In doing so you may wish to seek to consult and work with others outside of the EPS sphere e.g. social scientists, ethicists and public engagement experts.

Assessment

Assessment of proposals will take the form of a 2 stage process: (1) postal peer review and (2) prioritisation panel.

Stage 1: Postal peer review

Proposals will be reviewed via a batched approach to conventional peer review, where selected reviewers assess more than one proposal to allow direct comparison. If a proposal receives sufficiently supportive reviewers' comments they will go forward to stage 2 of the assessment process. In order to aid the peer reviewing applicants are asked to **nominate 3 potential reviewers (including at least 1 international reviewer**). Please do not suggest reviewers that may have a conflict of interest. Our policy on what constitutes a conflict of interest can be found here https://www.epsrc.ac.uk/funding/assessmentprocess/coi/

Please note: we reserve the right to sift reject any full proposals that we deem not to have received sufficiently supportive reviewers' comments at stage 1 and as such will not be competitive at stage 2 prioritisation panel.

Stage 2: Prioritisation Panel

If the reviews are sufficiently supportive, the proposal will be assessed and ranked by a panel based on the reviewers' comments and the applicant response, using the assessment criteria provided below. The panel will consist of cross-disciplinary researchers and will include relevant experts and users from across the digital economy area.

Assessment Criteria

Proposals will be reviewed and ranked according to the following assessment criteria:

- **Relevance to the objectives of the call:**
    - Demonstration of the importance of specific context or real world scenario being addressed.

- Demonstration of research challenge(s) being co-created by end-user(s) and exposure of potential beneficiaries to the research challenge and potential impacts.
- The level and quality of engagement and co-creation with project partners and across disciplines across the life span of the research project.

- **Quality of research, including:**
  - Novelty, relationship to the context, and timeliness
  - The ambition, adventure and transformative aspects identified
  - Appropriateness of proposed methodology
  - Synergy and added value of proposed research strands
- **National importance over a 10 to 50 year time frame including:**
  - Contribution of proposal to other research areas, societal challenges, success of UK economy, emerging industry
- **Potential research impact, including:**
  - Relevance and appropriateness of any beneficiaries or collaborators (e.g. upstream engagement/co-design)
  - Plans for dissemination and knowledge exchange
  - Plans for promoting cross-disciplinary culture.
- **Ability of applicant team to deliver the research, including:**
  - Track record of the team, the leadership quality of the Principal Investigator
  - Balance of skills of the project team and integration of different methodologies and approaches.
- **Resources and management, including:**
  - Effectiveness of planning and resource management strategy
  - Appropriateness of resources requested.

Standard EPSRC practices and procedures will be followed throughout the assessment process.

Information about the EPSRC peer review process and guidance for reviewers can be found at: https://www.epsrc.ac.uk/funding/assessmentprocess/review/

Key dates

Activity	Date

Activity	Date
Call Launched	11 August 2015
Brokerage Event	03 September 2015
Compulsory Intent to Submit deadline	14 September 2015
Closing Date – Full Proposals	13 October 2015
Prioritisation Panel	February 2016
Funding Decision	March 2016

Contacts

Jerome Ma, Digital Economy Theme
Tel: 01793 444117; jerome.ma@epsrc.ac.uk

Tracy Keys, Digital Economy Theme
Tel: 01793 444306; tracy.keys@epsrc.ac.uk

Claire Tansley, Digital Economy Theme
Tel: 01793 444540; claire.tansley@epsrc.ac.uk

John Baird, Digital Economy Theme
Tel: 01793 444047; john.baird@epsrc.ac.uk

If you experience any problems submitting the proposal through Joint Electronic Submission (Je-S) System please contact the Je-S System Helpdesk, JeSHelp@rcuk.ac.uk, 01793 444164.

We would also suggest applicants contact their University Research Office for advice and guidance on writing their proposals, and would remind applicants that clicking 'submit document' on your proposal form in Je-S initially submits the proposal to your host organisation's administration, not to EPSRC. Please allow sufficient time for your organisation's submission process between submitting your proposal to them and the call closing date.

Change log

Name	Date	Version	Change
Jerome Ma	09 July 2015	1	N/A
Jerome Ma	21 July 2015	2	