Job Title:	Research Fellow A

Responsible to:	Head of research group, or principal investigator

Responsible for:	Not applicable

Job Summary and Purpose:
To undertake research in accordance with the specified research project(s) under the supervision of the principal investigator.

Main Responsibilities/Activities
To undertake a range of research activities within a specified research area, assuming responsibility for specific areas of projects and making use of new research techniques and methods, in consultation with the research award holder or supervisor. This may include fieldwork, interviews, laboratory experimentation, critical evaluation and interpretation, computer-based data analysis and evaluation or library research. Using initiative and creativity to identify areas for research develop new research methods and extend the research portfolio. Analysing and interpreting results of own research. Write up results and prepare papers for submission to appropriate journals and conferences, and other outputs as required and/or appropriate. Attend appropriate conferences for the purpose of disseminating research results of personal development. The post holder may also contribute to writing bids for research grants and will contribute to collaborative decision making with colleagues in areas of research. Continually to update knowledge and develop skills, and translate knowledge of advances in the area into research activity. To plan and manage own research activity in collaboration with others. To carry out administrative tasks associated with specified research funding, for example risk assessment of research activities, organisation of project meetings and documentation. Implementation of procedures required to ensure accurate and timely formal reporting and financial control. To contribute to teaching in the Faculty by carrying out student supervision and/or demonstrating within the post holder's area of expertise and under the direct guidance of a member of departmental academic staff, as appropriate. The post holder may occasionally be required to supervise more junior research staff.

Person Specification
The post holder must have: A doctoral degree in a relevant discipline (although individuals who have almost completed a doctoral degree may be appointed). Consideration may also be given to individuals who do not hold a doctoral degree but have required skills based on a number of years experience in specified / relevant fields The post holder will have authority over some aspects of project work and must be capable of providing academic judgement, offering original and creative thoughts and be able to interpret and analyse results.

Relationships and Contacts
Direct responsibility to the principal investigator or academic supervisor. The post holder may be asked to serve on a relevant Faculty committee. There may be additional reporting and liaison responsibilities to external funding bodies or sponsors. The post holder may work on original research tasks with colleagues in other institutions.

Special Requirements
To be available to participate in fieldwork as required by the specified research project

All staff are expected to:

- Positively support equality of opportunity and equity of treatment to colleagues and students in accordance with the University of Surrey Equal Opportunities policy.
- Help maintain a safe working environment by:
  - Attending training in Health and Safety requirements as necessary, both on appointment and as changes in duties and techniques demand
  - Following local codes of safe working practices and the University of Surrey Health and Safety Policy
- Undertake such other duties within the scope of the post as may be requested by your Manager.

Role Purpose Addendum	Research Engineer (Research Fellow) in adaptive online safety and privacy software

Job Summary and Purpose:

This information sheet should be read in conjunction with the accompanying generic Research RA1A Role Profile and will be used for shortlisting processes. More specifically the post holder will be expected to:

(i) Design and develop software such as browser extensions, mobile apps, open-source software libraries and datasets to be released from the project to be produced and released by the "AP4L" project.
(ii) Collaborate with other staff on the project to develop pilot and proof-of-concept systems for: fundamental new privacy enhancing technologies, privacy sensitive machine learning to personalise automatic online safety responses and immersive simulation environments to explore how safety and can be compromised online during life transitions.
(iii) Work with other researchers on the project to facilitate reproducible research and public engagement.
(iv) Contribute to participative research engagement events and activities with stakeholders.
(v) Meet on a weekly basis with project staff, and attend project meetings and present results at other sites as required;
(vi) Publish and present research in high-quality international journals and conferences.
(vii) Pro-actively organise and manage own time and research-related activities.
(viii) Report orally and prepare papers reporting progress and delivery of project outcomes and be able to communicate at both technical and high-level for example with project research partners.
(ix) Perform any other duties associated with the project, as deemed appropriate to the grade by the Principal Investigator.
(x) Promote the research and activities of the project and the Distributed and Networked Systems (DANS) group and the Surrey Centre for Cyber Security (SCCS) in national and international forums as well as in cohort activities related to the REPHRAIN National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online.

Main Responsibilities/Activities

Undertake the development of research software for the AP4L, either using methods arising from research or to enable research to take place.

Meet on a weekly basis on campus with project staff and wider research groups (DANS and SCCS).

Attend project meetings and present results at other sites as required

Give oral and written reports on project progress and outcomes. Be able to report at both a technical low-level and conceptual high-level to a range of audiences including the public and industry

Continually update knowledge and develop skills

Carry out routine administrative tasks associated with a specified research project, for example risk assessment of research tasks, organisation of project meetings and documentation. This will entail planning own day-to-day research activity within the framework of the agreed programme, dealing with problems that may affect the achievement of research objectives and deadlines and implementing procedures required to ensure accurate and timely delivery.

Person Specification

The post holder must have:

- Master's degree in computer science or a related subject, or equivalent professional experience
- Software development experience relevant to online safety and privacy, using languages such as Python and JavaScript.
- Ability to develop web applications and mobile apps using state-of-the-art frameworks.

The post holder would ideally have:

- Experience developing Privacy Enhancing Technologies and Crypto Software is desirable.
- Skills and experience of development in machine learning and/or deep learning tools (TensorFlow, PyTorch, Keras, etc.) is desirable.
- Direct research experience in Online Safety and Privacy, Privacy Sensitive Machine Learning or Usable Security and Privacy is desirable, including developing new algorithms related to research.
- Strong writing skills across different levels of technical audience are desirable
- A track record of publishing academic papers, open-source software tools and/or research datasets is desirable

Relationships and Contacts

Direct responsibility to Principal Investigator Prof. Nishanth Sastry.

Informal enquiries are welcome and should be directed to Prof Nishanth Sastry, n.sastry@surrey.ac.uk

Additional Background Information

This post is part of an EPSRC project **AP4L: Adaptive PETs to Protect & emPower People during Life Transitions**, funded through the Protecting Citizens

Online Call 2. The aim of this project is to undertake research in online privacy & vulnerability challenges that people face when going through major life transitions such as relationship breakdowns; LBGT+ transitions or transitioning gender; entering/leaving employment in sensitive sectors such as the Armed Forces; and developing a serious illness or becoming terminally ill. (More details in the summary given at the end of this section)

.

The postholder will be responsible for designing and building the software to be developed in the project, such as browser extensions, mobile apps, open-source software libraries and datasets to be released from the project. The software to be developed will include fundamental new privacy enhancing technologies, privacy sensitive machine learning to personalise automatic online safety responses and immersive simulation environments to explore how safety and can be compromised online during life transitions.

The postholder will be part of a cohort of researchers working with the REPHRAIN National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online. A key aspect of the project is working closely with 26 core partners spanning legal enforcement agencies (e.g., Surrey Police), tech companies (e.g., Facebook, IBM), support networks (e.g., LGBT Foundation, Revenge Porn Helpline, Macmillans Cancer Care), financial agencies (Mastercard, Lloyd's) and regulators such as Ofcom. A six-part radio series has been commissioned by the BBC for disseminating the key project messages.

Relevant Research Environment in the Department

The postholder will be based in the Department of Computer Science, which has a world-class reputation in Cyber Security, Distributed and Networked Systems, and Nature Inspired Computing & Engineering, and regularly publishes at top-level conferences and journals.

The Surrey Centre for Cyber Security (SCCS) is only one of seven in the UK holding recognition as an Academic Centre of Excellence in both Cyber Security Research and Cyber Security Education by the UK government. SCCS has world-leading research expertise in applied cryptography, trusted computing, secure systems, privacy and authentication, secure communications, blockchain and distributed ledger technologies, and security verification.

The Distributed and Networked Systems (DANS) group is internationally recognised for its fundamental and applied research in several areas such as consensus protocols, distributed trust and coordination, fault-tolerance, edge and cloud computing, networks in space, web tracking and privacy, online harms such as hate speech and misinformation in social networks.

Several of the Project Investigators are also Surrey AI Fellows in the new Surrey Institute for People Centred AI, and also members of the Nature Inspired Computing and Engineering (NICE) group, which holds world-leading expertise in machine learning and AI, including trustworthy AI (explainable, secure and privacy preserving machine learning), systems biology, bioinformatics, image processing, natural language processing, computational neuroscience, computational optimization, AI planning and optimal control.

Project Summary: AP4L: Adaptive PETs to Protect & emPower People during Life Transitions

AP4L is a 3-year program of interdisciplinary research, centring on the online privacy & vulnerability challenges that people face when going through major life transitions. Our goal is to develop privacy-by-design technologies to protect & empower people during these transitions. Our work is driven by a narrative that will be familiar to most people. Life often "just happens", leading people to overlook their core privacy and online safety needs. For instance, somebody undergoing cancer treatment may be less likely to finesse their privacy setting on social media when discussing the topic. Similarly, an individual undergoing gender transition may be unaware of how their online activities in the past may shape the treatment into the future. This project will build the scientific and theoretical foundations to explore these challenges, as well as design and evaluate three core innovations that will address the identified challenges. AP4L will introduce a step-change, making online safety and privacy as painless and seamless as possible during life transitions

To ensure a breadth of understanding, we will apply these concepts to four very different transitions through a series of carefully designed co-creation activities, devised as part of a stakeholder workshop held in Oct'21. These are relationship breakdowns; LBGT+ transitions or transitioning gender; entering/ leaving employment in the Armed Forces; and developing a serious illness or becoming terminally ill. Such transitions can significantly change privacy considerations in unanticipated or counter-intuitive ways. For example, previously enabled location-sharing with a partner may lead to stalking after a breakup; 'coming out' may need careful management across diverse audiences (e.g - friends, grandparents) on social media.

We will study these transitions, following a creative security approach, bringing together interdisciplinary expertise in Computer Science, Law, Business, Psychology and Criminology.

We will systematise this knowledge, and develop fundamental models of the nature of transitions and their interplay with online lives. These models will inform the development of a suite of technologies and solutions that will help people navigate significant life transitions through adaptive, personalised privacy-enhanced interventions that meet the needs of each individual and bolster their resilience, autonomy, competence, and connection. The suite will comprise:

(1) "Risk Playgrounds", which will build resilience by helping users to explore potentially risky interactions of life transitions with privacy settings across their digital footprint in safe ways

(2) "Transition Guardians", which will provide real-time protection for users during life transitions.

(3) "Security Bubbles", which will promote connection by bringing people together who can help each other (or who need to work together) during one person's life transition, whilst providing additional guarantees to safeguard everyone involved.

In achieving this vision, and as evidenced by £686K of in-kind contributions, we will work with 26 core partners spanning legal enforcement agencies (e.g., Surrey Police), tech companies (e.g., Facebook, IBM), support networks (e.g., LGBT Foundation, Revenge Porn Helpline) and associated organisations (e.g., Ofcom, Mastercard, BBC). Impact will be delivered through various activities including a specially commissioned BBC series on online life transitions to share knowledge with the public; use of the outputs of our projects by companies & social platforms (e.g., by incorporating into their products, & by designing their products to take into consideration the findings of our project) & targeted workshops to enable knowledge exchange with partners & stakeholders.