Centre for
Digital Citizens

Citizen Challenge Area:

Safe Citizen

How can digital technologies support fair, secure and equitable societies?

We critically examine the safety & security challenges associated with online exchanges.

TEAM

Safe Citizen Leads: Professor Pam Briggs, Professor Aad Van Moorsel

Academic team: Dr Dawn Branley-Bell, Dr Kovila Coopamootoo, Professor Lynne Coventry, Dr Clara Crivellaro, Dr Yu Guan, Dr Magdalene Ng

OVERVIEW

The recent UK Online Harms White Paper highlights the ways in which citizens can be vulnerable to online threats in an increasingly digital world. It reflects the UK's aim to take a global lead in developing measures that support secure digital innovation. The harms defined in the report include abuse, bullying, fake news, radicalisation, and the psychological impacts of social media, but also point to a marked rise in sophisticated social engineering and ransomware attacks on businesses and citizens.

Other social harms are beginning to emerge in our increasingly sensor-based, data-rich society, where the source data and resulting algorithms reportedly feed systematic forms of bias into organisational and national decision-making. This means that the interests of the individual citizen can be overlooked in the transition to a digital society.

The Safe Citizen Challenge Area will explore how we can identify and mitigate the online harms that result from a reliance on largely unregulated digital communication. We will also explore how to identify and mitigate social harms that can emerge in new 'smart' interactions.

Get involved:

- Find out more by having a chat with the Safe Citizen Challenge Area leaders, Pam and Aad, or contact Rachel Pattinson, Centre Manager
- Share your project ideas! If you have an idea you'd like the Centre for Digital Citizens support with, we'd love to hear about it!
- Visit the website: www.digital-citizens.uk

Digital Economy
Transforming Business and Society

UKRI Engineering and Physical Sciences Research Council

Areas we're interested in exploring

Co-designing privacy and security technologies with diverse communities and for new settings: How can secure Blockchain technologies and new identity management systems be used to support communities? For example, these technologies could be used for distributing community vouchers or promoting civic/volunteer engagement, but will they be accepted and trusted by those same communities?

Can new privacy and security technologies improve access and data sharing for marginalised or remote and poorly connected communities, addressing issues of stigmatisation, citizenship across borders and harm reduction?

Understanding the social practices and dynamics of safe citizenship: What are the social practices and dynamics of security and privacy? How is privacy and security experienced and enacted in our families, communities, and organisations? We're interested to move away from the individual and to explore collective privacy and security within the home or community.

Responding to changing work practices: The COVID-19 pandemic has resulted in a huge change in work practices. The phenomenon of more remote distributed working means that people are less tied to place, so what are the implications of this? These new hybrid working models bring new threats: from organised crime, new forms of 'insider threats' and new privacy and security risks to the individual. How do we ensure that workers feel they belong to the organisation, have psychological ownership and behave securely?

Upskilling communities: A 'responsible security' approach to upskilling people and communities would mean working with communities to build resilience, co-design training or set up better networks to promote knowledge exchange around privacy and security. However, do we understand the requirements of 'upskilling' in communities and the power relations at play?

We aim to look at how diverse citizen experiences impact upskilling in communities and also consider the longer-term implications of being digitally isolated or being digitally 'better connected'.

Revealing the workings of technology: We can't be blindly accepting of computer-generated decisions. How can we best reveal the inner workings of technologies, so that we can generate improved transparency and promote deeper critical scrutiny, particularly around data privacy, security and trust? This might involve investigations of mental models, explainable AI, making the invisible computer visible, and other ways of improving public trust.

There is a link here to social justice, personal autonomy and critical thinking – in terms of how we support individuals to make more considered choices. In what ways is behaviour manipulated either for good or for bad by interface and system designs?

Examples of collaboration:

Two past projects illustrate our ways of working with partners: In the cSALSA project we worked with agencies supporting older adults (Age UK, University of the Third Age), setting up workshops to understand how, post-retirement, they access the skills and knowledge to stay safe online. In the FinTrust project, we work with Atom Bank, a challenger bank located in Durham, to investigate people's trust in digital banking and to improve inclusion in digitized banking across various segments of the population.