****

**Centre for Science and Policy**

**Cambridge Computer Laboratory**

**European Commission**

**Policy Workshop Report**

**Next Generation Internet**

**1 – 2 March 2017**

**Wolfson College Cambridge**

**Introduction**

The Centre for Science and Policy (CSaP) in collaboration with the Cambridge Computer Laboratory, organised a Policy Workshop in support of the European Commission’s (EC) Next Generation Internet (NGI) initiative.

This report has been prepared by Makoto Takahashi, CSaP Policy Intern, and captures the views and ideas generated by the participants during the workshop.

**CSaP Team**

* Jackie Ouchikh (Head of Programmes)
* Makoto Takahashi (Policy Intern)
* Steven Wooding (Lead for Research & Analysis)

**Background and purpose**

The EC’s NGI initiative, to be launched in 2018, will address both the technological and policy aspects of the future of the internet, in order to make it more "open" and "human". Preparation for this initiative is now underway, with an open online consultation and a series of workshops taking place across the EU. The range of issues to be explored is diverse, ranging from cybersecurity, artificial intelligence and the ‘Internet of Things’ to new decentralised approaches for data governance.

The purpose of the workshop was not to redesign the TCP/IP protocol. It was to brainstorm novel ideas and to have an open and multidisciplinary discussion of the approach the EC are taking in preparing for the launch. Topics for discussion included:

* the process (open consultations, engagement between policy and research)
* the type of topics (technology- / socially-driven)
* the tools to be used

**Next steps**

* The EC reflected that the workshop delivered on high expectations, providing a broad, complex and ambitious discussion over the course of the two days
* As it works toward its vision of a human-centred internet, the EC will continue to engage with workshop participants; offering them a concrete opportunity to influence European policy
* The EC would particularly welcome inputs such as papers or reports related to NGI, as well as blog posts or video messages for their webpage: [*https://ec.europa.eu/futurium/en/next-generation-internet*](https://ec.europa.eu/futurium/en/next-generation-internet).
* The EC also stressed its willingness to collaborate with participants in delivering further workshops, which are a key component of the effort to build an NGI ‘movement’

**Day 1**

The NGI workshop was hosted at Wolfson College, Cambridge over the course of two days. The session on 1 March took the form of a roundtable discussion, which aimed to identify key issues for more concentrated deliberation on 2 March. As the debate developed, key themes and comments were recorded using post-its and arranged on the floor to form a mind map; images of which are available in appendix (see: Appendix I – X).

**Programme**

16:15 Welcome (Rob Doubleday)

16:20 Introduction and background (Jesus Villasante)

16:30 Workshop outline (Steven Wooding)

16:45 What are the key issues for the NGI over the next 2 – 10 years?

* Each attendee to contribute 1-2 suggestions
* Suggestions are recorded and added to a mind map of key issues
* General discussion of the suggestions raised

18:45 Taxis to Christ’s College

19:00 Networking & drinks

19:30 Informal discussions continue over dinner

21:30 Close

**Discussion**

**Next Generation Internet**

* NGI aims to build a “human-centred internet” by shaping how new technologies (e.g. AI, Internet of things) are implemented in order to deliver tangible benefits to society.
* To deliver on this vision, the EC seeks to attract and collaborate with bright early-career researchers and tech start-ups, who are at the cutting edge of digital technology.
* Some participants questioned the utility of the term “next generation internet”, noting that it could be understood to suggest a shift from TCP/IP to new protocols.
* We were informed that the TCP/IP protocols designed by Cerf in 1973 – 1974 were based on two principles: (i) no one would own the network; (ii) network would be agnostic about content. These principles are understood to have established a “platform for permissive innovation”.
* It was asked if the NGI should affirm the internet’s founding principles or establish new ones; prompting a lively discussion about “European values”.
* Not all participants saw the value of discussing TCP/IP’s founding principles. The architecture of the internet may be permissive, but as many sites (e.g. Facebook, Twitter, Instagram, etc.) and laws are not, our experience of the internet does not embody these values, it was argued.
* It was concluded that it may be more meaningful to discuss how the EC could shape “digital society” rather than the “internet” itself. This language could help emphasise the human-centred nature of NGI, including the need to invest in education and skills.

**Concentration of data and power**

* Participants criticised the idea that the internet is inherently libertarian and disruptive, offering Google and Facebook as examples of industrial consolidation.
* Repeated references were made to Professor Tim Woo’s “*The Master Switch*”, which chronicles how the telephone, radio, cinema and television were hailed as vehicles of social disruption, before falling to corporate monopolisation.
* Concern was voiced about the concentration of data on a few platforms (e.g. Facebook, Google, etc.), which will place them in pole position to make use of emerging AI technologies and further entrench their market dominance.

**Visible AIs**

* As machine learning advances, AI will play an increased role in daily life (e.g. self-driving cars, semi-automated justice systems).
* The prominence of AI will pose new ethical questions, as well as creating a new and urgent demand to answer old ones. For example, self-driving cars will face the classic “trolley problem”, which involves choosing a course of action where every option leads to harm.
* We heard that there is a need for AI to be transparent, so that citizens can understand how their personal data is being used.
* But the complexity of systems where multiple AI interact will make it difficult to achieve meaningful transparency.
* Participants provocatively proposed the idea of rights for AI; arguing that if AI were to be taxed, as Bill Gates’ had suggested, they could be afforded civil protections under the principle of “no taxation without representation”.

**Safety**

* The proliferation of AI and the internet of things has the capacity to deliver enormous benefits to society, but will also create new risks.
* Cyberphysical attacks and AI terrorism will be among the new threats that the state has to manage.
* Making companies responsible for providing security updates over the long term could mitigate some of these risks. The example of a self-driving car, produced and purchased in a developed nation, before being sold second-hand to a developing nation was raised. It was argued that NGI could aim to ensure that security updates are provided for the entirety of the car’s use, not just its use by the initial purchaser.

**Role and nature of the State**

* In the 1980s and 1990s, utopian thinkers claimed that states could not govern the internet (e.g. John Perry Barlow’s “*Declaration of Independence of Cyberspace*”).
* Contrary to these claims, the internet is heavily regulated and subject to state influence (e.g. the NSA’s PRISM program, the Great Firewall of China, etc.).
* Governments will continue to have an important role in regulating the internet and ensuring prosperity.
* States are creating geographies of data through data localisation laws, which require companies to store customers’ and employees’ personal data locally.
* NGI could develop new models of citizenship. Estonia’s electronic-ID system could be implemented across Europe, enabling free access to all state services, participants suggested; coining the term “à la carte citizenship”.

**Legislative Speed**

* Technical innovation often progresses faster than the passage of new legislation, we heard.
* Using AI to automate some of the legislative process could be one way of helping the law to match the rate of technological change.
* Other participants questioned if accelerating the legislative process should be an NGI objective, pointing out that the internet is already heavily legislated. It may be more important to find new ways to enforce existing laws, they argued.
* It was agreed that investing in hybrid teams of lawyers and technical experts will help ensure that legislation is relevant and implemented effectively.

**Social Dynamics**

* We heard that the internet is “flattening” and “widening” our social architecture; meaning that we have a growing number of increasingly shallow interactions.
* Using the language of the “social contract”, participants asked if innovators are responsible for the impacts of their products on social dynamics.

* The potential for AI to provide free and accessible education should be promoted by NGI.
* Preserving “free” choice in a system of complicated algorithms was raised as a future challenge.
* The rise of “post truth” politics underscores the importance of access to reliable information. Participants debated the ethics and practicalities of “popping information bubbles” by regulating social media and targeted advertising, with reference to the principle of net neutrality.
* It was agreed that any interventions that are made should be informed by research into human psychology, and recognise that we may have a bias toward preserving our bubble.

**Access**

* Differential access to internet services will continue to be a problem. NGI could attempt to address this issue through a number of strategies, including subsidies for the least able to afford internet access and universal free Wifi.
* Security concerns were agreed to be a serious barrier to personal internet access. One strategy for mitigating concern could be a shift from the model of “security as a private responsibility” (i.e. one in which citizens purchase anti-virus software as individuals) to a model of collective internet security, in which the state assumes responsibility for providing or subsidising security software.
* Participants also noted that the NGI will need to consider its impact on non-EU citizens and their experience of the internet.

**Day 2**

The workshop on 2 March aimed to develop the discussion from 1 March, and distil a series of concrete aims and suggestions for the EC’s NGI initiative. The day’s activities were structured around three questions:

1. What should the NGI do?
2. How can the EC achieve these aims?
3. Who are the stakeholders in NGI? And what are the early indicators of success or failure?

**Programme**

09:00 Welcome

09:15 Introduction to purpose of workshop (Jesus Villasante)

09:30 Summary of day 1 and plan for day 2 (Steven Wooding)

09:45 Session 1: “*What should the NGI do?*”

10:40 Perspective talk (Lorna Woods)

10:45 Coffee

11:00 Session 2: “*How can the EC achieve these aims?*”

12:10 Perspective talk (Lucie Burgess)

12:15 Lunch

13:15 Session 2 (feedback session)

14:10 Perspective talk (Lani Cosette)

14:15 Tea

14:30 Session 3: “*Who are the stakeholders in NGI? And what are the early indicators of success or failure?*”

15:45 Wrap up & next steps (Jesus Villasante and Peter Fatelnig)

16:15    Close

**Session 1: What should the NGI do?**

Building on Day 1, this session aimed to identify key objectives for the NGI. Participants were invited to make suggestions, which were recorded on flipcharts. At the end of the session, each attendee was handed three stickers and invited to vote on the objectives they considered most important. The results of the vote are recorded below:

* Avoid the concentration of power 17
* Promote broader access 13
* Promote sovereignty over personal data 13
* Promote access to data as a common good 11
* Promote public goods (commons) 9
* Promote a la carte citizenship/subsidiarity 8
* Promote and facilitate choice 5
* Promote a balance between virtual and physical lives 5
* Enhance economic welfare 4
* Promote diversity 3
* Promote cyber-security as a public good 3
* Promote net neutrality 3
* Avoid the concentration of wealth 3
* Establish appropriate regulatory regimes 2
* Promote cyber-physical security 1
* Establish individualised trusted intermediaries 1
* Promote open intellectual property 1
* Promote the right to disassociate 1

**Session 2: How can the European Commission achieve these aims?**

Small groups were organised around the most popular objectives identified in Session 1: (i) broadening access; (ii) à la carte citizenship; (iii) promotion of public good; (iv) sovereignty over personal data vs data as a public good; (v) preventing the concentration of power. Each group was then asked to discuss the objective with reference to: technical feasibility; legislative tools that the EC could use; and potential barriers. Groups recorded their discussions using flipcharts, images of which are available in the appendix (see: Appendix XXI – XXII).

**Group 1: Broadening access**

* NGI should conceive of the internet as the “fourth utility”, in recognition of its ubiquitous use and central role in accessing state services (e.g. NHS Choices).
* NGI could uncouple bandwidth from income by implementing a “TV-licence model” of internet access, based on the principle of a single fee and a single level of service.
* “Access” was interpreted as referring to how the internet will transform access to societal goods (e.g. work), not just access to the internet itself.
* Participants echoed Bill Gates in suggesting a tax on AI. The funds raised could be invested into retraining those that AI will make redundant.
* The EU’s role in access to online services (e.g. Facebook) remains unclear. These spaces are private, but are treated as though they were public. Shopping malls were raised as an analogue corollary to this debate.
* Access is not just a technical issue - it is also social. Education schemes could build the trust and technical literacy necessary for access.
* Trust can also be built by making the rights of citizens over their data clear. Participants suggested that the NGI promote the “right to be forgotten” and the right to opt out of data collection.
* Language will continue to be a barrier to access. NGI should aim to ameliorate this issue, possibly by supporting automated translation.
* Recognising that personal data plays a vital role in optimising services, it was suggested that “donating” personal data to institutions could be reframed as a civic responsibility, or a “payment” for access to specific service.

**Group 2: à la carte citizenship**

* The group’s concept of “à la carte citizenship” was inspired by Neal Stephenson’s *Snow Crash*. Published in 1992, the novel describes an anarcho-capitalist society, where most services have been marketised and digital currency has largely supplanted notes and coins.
* Drawing on Stephenson’s work, the group envisaged Europe’s conversion from the euro to a new digital currency: the e-Onion. This possible future served as a thought experiment to generate new ideas.
* In this possible future, all citizens would be issued with an e-ID at birth. The proposed e-ID is modelled after Estonia’s e-residency scheme and would allow access to state services across Europe. This would enable EU citizens to move across Europe with greater ease, and enable free choice of services (e.g. healthcare, education, etc).
* NGI could foster trust in government by promoting the use of smart contracts, participants suggested; coining the term “blockchain governance”. This possibility is currently being explored by the UK’s Department of Work and Pensions.
* NGI could establish “personal clouds”. Each cloud would store all of a single individual’s data. Citizens could allow access to their cloud in exchange for services, creating a two-way market.

**Group 3: Promotion of the public good**

* NGI will have to weigh the benefits of increased internet access against its environmental cost, participants cautioned; noting that the network already accounts for 10% of the UK’s energy consumption.
* The environmental impact of digital innovation is often invisible, making it difficult to regulate. How did Facebook’s decision to make videos play automatically affect energy consumption, for example? And how could Facebook be held accountable?
* NGI could reframe cybersecurity as a collective good, instead of a private responsibility. This would be consistent with national defence, policing and immunisation against disease.

* The importance of collective security is illustrated by the rise of “credential stuffing” incidents, such as the 2016 O2 hacking. Exploiting the fact that many people use the same password on multiple sites, hackers gained access to thousands of O2 customers’ details by breaching XSplit: a relatively weakly protected gaming site.
* Collective digital security could take the form of subsidies for the least able to invest.
* It was suggested that attempts to promote collective security could be undermined by the free-rider problem.

* Governments may also lack the expertise necessary to promote collective security.
* Access to information and knowledge is a universal good and could be promoted by subsidising news and academic publishing.
* However, promoting greater access to news outlets does not resolve issues surrounding the integrity of the information they are publishing.
* Group 3 echoed Group 1 in arguing that NGI should promote internet access as a public good. It was suggested that this could be achieved by investing in infrastructure to provide free Wifi.

**Group 4: Sovereignty over personal data vs data as a public good**

* Participants proposed a broad definition of “personal data”, that includes not just data produced by the individual (e.g. Facebook posts, emails) but data collected about the individual (e.g. internet footprint, satellite footage)
* Participants also clarified that they were interested in the use of data for the public good, rather than data as a public good.
* NGI could promote sovereignty over personal data, through mechanisms such as a legal “right to be forgotten”.
* It was recognised that data sovereignty is in tension with the use of data to promote the public good (e.g. use of patient metadata to provide more efficient healthcare)
* One possible compromise is to legislate the use of personal data, ensuring it can be used for essential services (e.g. healthcare) but not for profit.
* The NGI will also have to establish the limits of data sovereignty. If someone aggregates and transforms data - for example - does this meta-data belong to them? Or is it still the property of the individuals who contributed the data?

**Group 5: The concentration of power**

* Participants warned that a handful of companies (e.g. Facebook, Amazon, Google) could establish monopolies on data.
* This would enable these companies to best exploit advances in machine learning, further enhancing their competitive advantage and establishing a positive feedback loop.
* Economies of scale could also contribute to locking in the competitive advantage of these companies.
* One means of preventing digital monopolies from emerging would be to cap the number of customers they can service (e.g. a cap on total Amazon Prime accounts), but this is politically unviable.
* Concern was voiced that preventing the concentration of power falls under the remit of antitrust agencies, which have a limited understanding of this sector. NGI could address this issue by investing in developing multi-disciplinary teams, with a cutting edge understanding of legal and technical issues.
* Promoting transparency is key to ensuring that legislation is enacted effectively, and data is not misused. But the difficulty of explaining AI systems to a general audience poses a challenge to making transparency meaningful.

**Session 3: NGI stakeholders and early indicators of success/failure**

The final session of the workshop was divided into two debates. The first concerned stakeholders in NGI. Participants were asked to evaluate how well engaged each stakeholder group was, and suggest strategies to foster engagement where it is lacking. In the second discussion, participants sought to discern what the early indicators of success or failure for the NGI might look like, as well as identify pertinent lessons from history. The discussions were recorded on flipcharts, images of which are available in the appendix (see: Appendix XXIII – XXVIII).

**Session 3a: Stakeholders in NGI**

**Engaged stakeholders:**

* Governance leaders
* Online platforms
* ISPs
* Mobile operators
* Regulators
* Device manufacturers
* Digital rights groups
* Military
* Police

**Questionably engaged stakeholders:**

* Academics
* Security companies
* Materials and suppliers
* Civil Society
* Foreign governments

**Unengaged stakeholders and possible strategies for engagement:**

* Early-career researchers
	+ Prizes/competitions
	+ Incubators, where they can collaborate with event organisers, advertisers, etc. to deliver impact
	+ Ring fencing funding
	+ Providing data sets
* Young people
	+ Model EU
	+ Popular culture (e.g. Robot Wars inspired children to become engineers)
* Gamers
	+ Art
	+ Social media
	+ Events and groups (e.g. meetup.com)
	+ Blogs of thought-leaders
* Start-ups
	+ Send visiting fellows
* Small and Medium Enterprises (SMEs)
	+ Prizes/competitions
	+ Providing infrastructure for growth
* Disenfranchised
	+ Celebrity endorsement
	+ Invest in European internet presence (e.g. social media)
	+ Promote net neutrality
	+ Invest in translation systems
	+ Presence in communities (e.g. townhall events)
	+ Art and popular culture
	+ Travelling exhibitions

**Session 3b: What are the early indicators of success/failure?**

**Indicators of success**

* More accurate expectations of privacy
* More accurate expectations about the use of personal data
* Greater variety in sources of information (e.g. it is currently estimated that Facebook and Google account for 80% of traffic to news sites)
* Rising number of companies in the internet sector (as an indicator of innovation)
* Creation of new jobs and greater value
* Technology used to tackle new problems (e.g. AI used to farm previously unused land)
* Public debates keep pace with developments in technology

**Warning signs**

* Increased opacity in how personal data is used
* Increased disengagement from digital society
* Scandals concerning data use reported by the media
* Destruction of jobs and value
* Aggressive patent enforcement (as an indicator of stagnation)
* Media mergers
* Continued proliferation of “fake news”

**Lessons from history**

* Any system will have “free-riders”
* Cognitive biases drive politics and should not be ignored
* Controversies can develop around new technologies (e.g. GM foods), leading to a loss of public confidence
* There is a price to “free”
* Issues surrounding pollution and shared resources indicate the need to engage a “global public”

**Conclusion**

This workshop was not structured to generate a list of key conclusions. Nevertheless, an attempt to pick out a short selection of salient themes and actionable suggestions has been made below.

**Key themes:**

* *Transparency*: Participants did not object to the use of personal data per se, but emphasised that users should understand how data is collected and processed, and to what ends. Recognising the value of personal data in optimising services, participants proposed a future in which individuals “donate” or “pay” for access to services with their data.
* *Concentration of data and power*: The concentration of data on a handful of online platforms (e.g. Google, Facebook, etc) places them in a prime position to exploit advances in machine learning, further locking in their competitive advantages. It was noted that anti-trust agencies will be responsible for preventing the emergence of monopolies, but have limited expertise in the technological sector. Investing in developing this capacity is therefore a priority.
* *Sovereignty over personal data*: There is a clear tension between the desire to promote sovereignty over personal data and the potential benefits that data analytics can deliver (e.g. optimising healthcare, preventing crime, etc.). It was particularly clear that there is a need to establish whether meta-data is owned by the individuals who have contributed their personal data, or the person who has aggregated and transformed the data.

**Actionable suggestions:**

* *e-ID*: Repeated references were made to up-sizing Estonia’s model of e-citizenship to the European scale. This would allow EU citizens greater freedom of movement and choice of services.
* *Collective online security*: A transition from private online security (i.e. purchasing security software individually) to collective online security (i.e. the state provides or subsidises security software) would lower barriers to access. This would also be consistent with our understanding of physical security.
* *Multi-disciplinary teams*: Investing in drawing technical experts into legal institutions generally, and antitrust agencies specifically, was suggested as essential to ensuring that these organisations are effective.

**Contributors**

* **Dr Anne Alexander,** Co-ordinator, Digital Humanities Network, Centre for Research in the Arts, Social Sciences and Humanities, University of Cambridge
* **Professor Ross Anderson,** Professor of Security Engineering, Computer Laboratory, University of Cambridge
* **Dr Andres Arcia-Moret**, Research Associate, Computer Laboratory, University of Cambridge
* **Professor Jean Bacon**, Professor Emerita of Distributed Systems, Computer Laboratory, University of Cambridge
* **Ted Barry,** Senior Policy Officer, Cabinet Office
* **Katja Bego**, Data Scientist, Technology Futures Team, Nesta
* **Lucie Burgess,** Head of Personal Data and Trust, Catapult and Senior Research Fellow, Hertford College, University of Oxford
* **Guy Cohen**, Strategy and Policy Lead, Privitar Ltd
* **Lani Cosette,** Director, EU Government Affairs, Microsoft Europe
* **Professor Jon Crowcroft,** Professor of Communications Systems, Computer Laboratory, University of Cambridge and CSaP Associate Fellow
* **Richard Dent,** PhD student, Department of Sociology, University of Cambridge
* **Professor David De Roure,** Director, Oxford e-Research Centre, University of Oxford
* **Mark Devereux,** Senior Principal, Promontory Financial Group
* **Dr Raluca Diaconu,** Research Associate, Computer Laboratory, University of Cambridge
* **Dr Robert Doubleday**, Executive Director, CSaP
* **Peter Fatelnig**, Deputy head of unit, CONNECT E3 Next Generation Internet, DG Connect, European Commission
* **Jorge Gasos,** Programme Officer, CONNECT E3 Next Generation Internet, DG Connect, European Commission
* **John Grant,** Owner,Ninetiles
* **Dr Garrick Hileman**, Senior Research Associate, Centre for Alternative Finance, Judge Business School, University of Cambridge
* **William Janeway,** Senior Adviser and Managing Director, Warburg Pincus
* **Dimitra Kamarinou**, Research Assistant, School of Law, Queen Mary, University of London
* **Dr Johannes Klinglmayr,** Senior Engineer, International Projects, Sensors & Communication, Linz Center of Mechatronics GmbH
* **Professor Neil Lawrence,** Professor of Machine Learning and Computational Biology, Department of Neuroscience, University of Sheffield
* **Dr Pietro Lio,** Reader in Computational Biology, Computer Laboratory, University of Cambridge
* **Professor Christopher Marsden,** Professor of Media Law, Sussex Law School, University of Sussex
* **Professor Christopher Millard,** Professor of Privacy and Information Law, School of Law, Queen Mary
* **Dr Brent Mittlestadt,** Postdoctoral research fellow, Oxford Internet Institute, University of Oxford
* **Jessica Montgomery**, Senior Policy Adviser, The Royal Society
* **Dr Ken Moody,** (retired) Reader in Distributed Information Management, Computer Laboratory, University of Cambridge
* **Professor John Naughton**, Emeritus Professor of Public Understanding of Technology, The Open University
* **Dr Magda Osman,** Senior Lecturer in Experimental Cognitive Psychology, School of Biological and Chemical Sciences, Queen Mary, University of London
* **Joerg Ott**, Professor for Networking Technology, Department of Communications and Networking in the School of Electrical Engineering at Aalto University
* **Andrea Passarella**, Researcher, Institute for Informatics and Telematics, National Research Council of Italy (CNR)
* **Dr Julia Powles**, Researcher, Faculty of Law, University of Cambridge
* **Professor Tom Rodden,** Professor of Computer Science, Faculty of Science, University of Nottingham
* **Dr Jatinder Singh,** Senior Research Associate, Computer Laboratory, University of Cambridge
* **Makoto Takahashi (note-taker),** CSaP Policy Intern and PhD Student, Department of Geography, University of Cambridge
* **Isabel Thornton**, PhD Student, Department of Sociology, University of Cambridge
* **Michael Thornton,** PhD Student, Department of History & Philosophy of Science, University of Cambridge
* **Dr Laurissa Tokarchuk,** Lecturer, School of Electronic Engineering and Computer Science, Queen Mary, University of London
* **Georgios Tselentis,** CONNECT E3 Next Generation Internet, DG Connect, European Commission
* **Alex van Someren**, General Partner, Amadeus Capital Partners, Ltd
* **Michael Veale,** PhD student, Department of Science, Technology, Engineering and Public Policy, University College London
* **Jesus Villasante**, Head of Unit, CONNECT E3 Next Generation Internet, DG Connect, European Commission
* **Dr Sandra Wachter,** Researcher in Data Ethics, Alan Turing Institute
* **Dr Adrian Weller,** Senior Research Fellow, Department of Engineering, University of Cambridge
* **Dr Damon Wischik**, Computer Laboratory, University of Cambridge
* **Dr Steven Wooding (workshop facilitator)**, Lead for Research and Analysis, CSaP
* **Professor Lorna Woods**, Deputy Director of Research (Impact), School of Law, University of Essex