THE CITIZEN - NEGOTIATING LIFE IN THE DIGITAL WORLD

> *“Are we going to continue on the road and just allow the governments to do more and more and more control - more and more surveillance? Or are we going to set up something like a Magna Carta for the world wide web and say, actually, now it's so important, so much part of our lives, that it becomes on a level with human rights?”*
>
> *"Unless we have an open, neutral internet we can rely on without worrying about what's happening at the back door, we can't have open government, good democracy, good healthcare, connected communities and diversity of culture. It's not naive to think we can have that, but it is naive to think we can just sit back and get it."*

Tim Berners Lee on BBC Radio, Mar 2014.

Scope of the Conference

The Enlightenment movement of the 18th Century marked a shift in individual-state-enterprise relationships. Today the Digital Enlightenment movement aims to achieve a better understanding of the ways in which individuals, governments and enterprises are redefining their relationship through the use of technology.

The theme of this year’s conference was: the individual (in her many societal roles) in relation to the ever increasing dimensions of the technological (digital) environment. We brought together a range of views: technologists, anthropologists, engineers, social scientists, entrepreneurs, designers, policy makers and leaders of civil society organisations in order to gain an increased understanding of how humans engage with digital life and which options emerge.

Given the rapid pace at which non-anticipated technological innovations develop and swiftly get integrated into peoples’ lives, new ways of thinking and talking about the role of ‘digital life’ are required, thus allowing people to have a complete and correct understanding of what their real options are and to help develop meaningful forms of accountability, transparency and regulation of data processing, that can keep pace with the ‘bit per second’ lives of individuals today.

Digital Enlightenment Forum (DEF) aims, through these new ways of thinking, to develop proposals for how best to move forward with a focus on inter-relation between individuals and the technological environment.

Wednesday 25th March 2015 - Research and Innovation technology projects in societal perspective - report

The 3rd Digital Enlightenment Forum (DEF) was hosted in Kilkenny, Ireland by the Telecommunications Software & Systems Group (TSSG) of the Waterford Institute of Technology (WIT). The opening day presented a unique and successful opportunity for individuals and organisations working across disciplinary lines to come together and discuss how citizens negotiate life in the digital world.A range of speakers made presentations on projects and initiatives exploring this field, showcasing the results achieved and the efforts that are being made. (See below for details and links to presentations.) In so doing, they illustrated the significant steps being taken to better understand how the future relationship between individuals and the technological environment define our experiences of what it means to be human, how we engage with others, and the type of society we are constructing. In thinking about this potential future, presenters and participants reflected on new and emerging areas of research that require investigation and exploration.

Throughout the day the paradigm of Responsible Research and Innovation (RRI) was drawn upon to consider what interventions could be made to positively shape the role of the digital world in the lives of citizens. Through this lens presenters explored many themes. Among these is the importance of cross-disciplinary collaboration, not only in spirit or in the carrying out of research but also in the practice of writing and presenting. It was also clearly recognised that the vitality and strength of RRI relies on a continuing search for new and innovative concepts. Furthermore it was clear that one of the most productive ways for these tools to emerge is through these forms of collaboration, and, in so doing, provide new means of understanding how individuals use and engage with technology.

In support of the development of new conceptual tools, and the wider construction of a toolkit, was the call to develop a narrative of what it means to act and be responsible, beyond a threshold of simple compliance. This call is being met in two main ways. The first is to educate and raise awareness among technology designers and developers on the ways in which they can actively enhance user experiences of technology, focusing on taking a citizen-centric approach to technology design. The second is to educate and raise awareness among users, to develop what has been described as a digitally literate society. Such a society would create a space for users to come to grips with the social and political structures that influence the ways we engage with and use technology.

One of the most pressing issues that emerged over the course of the day was the repeated recognition that action is required. As the boundaries between on- and offline lives continue to blur, the speed at which technologies are developing increases, and the innovative ways in which they are being put to use multiplies, the resounding impact they have on the ways we experience our sense of self and others is greater than ever before. The need to act in response to this was a common thread among the discussions that took place over the course of the day.

Out of this call to action a number of future steps and areas for further research were identified and suggested. Foremost among these was the potential for DEF to operate as a space within which alternative narratives of understanding can be explored. In light of the ways in which technology works to structure our space of abilities, the need to consistently question and widen our imaginaries was emphasised.

Within these activities emphasis was placed on giving equal recognition and voice to the concerns of all actors. In order to achieve this, continued critical engagement and reflection on how the paradigm of RRI develops and is deployed is required. In particular attention is needed to develop a meaningful understanding of the terms accountability, transparency and trust. This is especially important as RRI aims to establish practices that translates these values into practical actions and decision-making processes.

In this sense, DEF has the opportunity to develop its status as a space for fostering creative partnerships and research through the bringing together of the extensive experience and expertise it holds in its network of members. It is through frequent opportunities for critical exploration of emerging research paradigms, which DEF promotes and supports, that we can begin to develop and the new and emerging technologies that shape the world in which we live today.

Thursday 26th March 2015 - The Citizen: Negotiating life in the digital world - report

VIDEOS OF KEYNOTES ARE AVAILABLE ON OUR YOUTUBE CHANNEL.

The day was opened by the president of DEF **George Metakides**. He addressed the difficulties the citizen has in today's digital world to "negotiate", in the sense of "have a discussion with a view to compromise".

But with whom exactly is the citizen supposed to negotiate? Governments, who appear to have taken up almost total surveillance using new technologies? Or the fewer than ten leaders (the "digital oligarchs"), of giant companies which are the major collectors and traders of personal data on the Web. The Web was created for sharing among peers of comparable power, but it did not really work out this way. We need change.

He introduced the three main themes of DEF 2015: Liberty and Security; Education and Skills; and Ethics in the digital world and made an urgent call for action of the citizen.

The next keynote was given by **Minister Dara Murphy** (Minister of State at the Depts of the Taoiseach and Foreign Affairs with Special Responsibility for European Affairs and Data Protection).

Referring to the introduction he saw the DEF 2015 title and themes as a clear reminders of the role of politicians to assist and support citizens with the societal changes due to digitalisation. His role in the Irish government is to recognise the legitimate concerns of citizens to regain control on their data, and to coordinate all government actions on Data Protection and Privacy. The government's strategy focusses on improving the efficiency of government by:

- Sharing and integrating the ICT infrastructure
- Continue to improve the digital government servicing to citizens
- Improving and broadening governance
- Improving ICT resources
- Facilitate lawful response to the sharing of data.

He is confident that the long due new regulation on DP will be agreed this year in the EU Council, realising the need for consensus despite conflicting rights and views based on different cultures. The Irish government works at strengthening the DP Commissioners office and is establishing a multidisciplinary Data Forum for advising his department. He welcomes DEF's observations and advice.

Paul Timmers (Director Sustainable and Secure Society in DG CNECT, EC) addressed the EC view and actions on Cyber Security and Data Protection. The instruments available to the EC are:

1. Education towards a culture of cyber security and data protection and awareness of users of risks and potential.
2. Research and Innovation in the field through Horizon 2020.
3. The Directive on Network and Information Security based on developing: common requirements across Member States; EU-level cooperation between stakeholders; Risk management and reporting across sectors.
4. Proposed Data Protection Regulation to update the Directive of 1995, expected to be adopted end of 2016.

The EC strategy focusses on: bringing the Cyber Security capabilities and cooperation to maturity; developing a comprehensive policy framework to protect personal data, and making the EU world leader in handling Cyber Security.

Peter Paul Verbeek (Twente Univ, NL) discussed the topic from a techno-philosophical angle. He discussed the technologies of the self in the digital age and pleaded for a mediation approach. This would need understanding of human – technology relations, addressing the ethics of technology and from within technology.

Technology mediates the relation between humans and their environment, raising questions on artefacts and morality, the role of intentionality and moral mediation. It would lead to “ascetic design” with elements: not yes or no, but how; from assessment to accompaniment; critical use of technology; value-sensitive design; and governing mediation.

Gerard Corcoran (Huawei Ireland) took the enterprise perspective. He presented the drivers for innovations in networking and the vision of Huawei to achieve a better connected world. He discussed this for a Smart City Internet of Things application project that addressed many aspects, incl. buildings, transport, health, media and industry.

TJ McIntyre (UCD and Digital Rights Ireland) discussed legal questions in the digital world. He started with a quote that a seamless global-economic zone calls the nation state into question and followed on with three possible strategies to achieve certain control over the Internet. (1) The Internet architecture to be remade using the principle of “Code as Law” from Lessig. (2) Gatekeepers to be listed and given an intermediation task. (3) Self-regulation harnessed by the state. For all three he discussed the consequences, incl. the positive potential, the problems to be solved, and the risks for censorship and privacy intrusion.

Muirne Laffan (RTE Digital) discussed the empowerment of the citizen in a digital media world. The citizen has enormous access and freedom to choose what, when and how to consume content. It gives them strong control on the media, being independent and content creators themselves. Citizens work across multiple social platforms, constantly consuming, interacting and engaging, possibly at a global level. The role of the media has dramatically changed and she explained how RTE deals with this.

Following these keynotes the discussions took place in breakout sessions on the three topics indicated by the president.

1. Liberty & Security

Chairs: Laurence Millar & Thomas Gross; Rapporteurs: David Duque Anaya & Eileen Murphy.

Challenges

A range of participants came together to identify and discuss the challenges associated with researching the themes of liberty and security. In doing so they discussed a wide variety of issues and questioned some widely accepted assumptions about how the relationship between liberty and security is imagined.

Over the course of the breakout session a number of questions were raised regarding how we can define and best understand both liberty and security, and also liberty in relation to security.

As an important starting point it was noted that there are two lines along which we can understand liberty. The first being liberty as a negative normative value, where you are free **from** certain constraints and restrictions. The second is liberty as a positive normative value, where you are free **to** act in certain ways. Building on this dual understanding of liberty, there was extensive discussion on the need to recognise that we cannot understand the relationship between liberty and security as one of balance or trade-offs, but rather they are mutually constitutive and each requires the other to operate.

Further discussion on how to better understand what we mean by the term security explored the tensions between individual and collective or societal security. There was general agreement that you cannot think about the relationship between liberty and security without thinking about the role of the individual. Recognition was also given to the growing discourse of the collective good, and the increasing value placed on putting the collective good above and before that of the individual. Consideration was also given to the ways in which this discourse is increasingly framing the discussion on the relationship between liberty and security and closing down possible alternative avenues for thinking and exploring this relationship. Two further points were offered on the relationship between liberty and security. Firstly, the question was raised; can we say that liberty stops where it endangers society? Such an approach would require a contextual definition of liberty. Secondly, discussion branched out to consider defining liberty and security, and their relationship to one another, in terms of their relationship with the future. Specifically, security is seen as an attempt to construct a relationship with a certain imagined future, whereas, liberty is seen as an attempt to construct a relationship with an uncertain imagined future.

While the theme of the session was liberty and security a number of associated issues were also discussed. These included the role of privacy, without the right to which, it was described, you cannot really be free. Similar to liberty and security, privacy is also viewed as a term whose definition is context dependent, as individuals and groups engage with and determine a sense of privacy in a fluid way, adjusting from what and from whom they want things to be private.

In addition the issue of informed consent was discussed and the question of whether it is possible to achieve meaningful informed consent in a time that is characterised by 'tick the box terms and conditions' lifestyles was raised.

Building on these discussions of privacy, the topic of surveillance was raised. Anchored around the Snowden revelations, participants debated whether or not we are witnessing a chilling effect on the ways in which people engage with data gathering devices. For some participants there has been such an effect, but others did not agree. It was suggested that research should be done to gather empirical data on changes in behaviour regarding levels of awareness of surveillance post Snowden.

This in turn, opened the discussion to consideration of the different parties that are involved in constructing and shaping how the wider public understands surveillance technologies and techniques. Three key actors were identified, the individual, society and digital oligarchs. It was argued that we need to better understand what incentivises these parties in relation to privacy, liberty and security, and how can we best align their incentives..

Finally, many of the themes that were raised on the Wednesday of the conference emerged within the space of the session, with particular emphasis placed on the need to build relationships of trust, and how to operationalise an ethos of accountability.

Solutions

Special attention was given to the role DEF can play in furthering our understandings of the relationship between liberty and security. In so doing a number of points were raised.

Foremost among these was the need to critically identify and explore the forces that construct the relationship between liberty and security as one of opposition. This would require an unpacking of the way in which individual and collective security has been constructed.

These aims raised a number of questions, such as what can we do to change the oppositional relationship, what kind of environment is required to challenge this discourse, in addition to how can we best understand liberty in an era of unending, low impact threats.

In response to these questions a number of suggestions for the role DEF can play were put forward. These included the capacity for DEF to act as a space to develop the stories that don't get told. In this sense, DEF could act as a curator of debate on how Civil Society Organisations can hold governments to accountability. Two existing web-based initiatives were offered, 'They work for you' and '38 degrees' as models for exploring possible future steps.

Additional actions DEF could take include an exploration of concepts and linguistics bundles that frame the narratives that develop around liberty and security. Such a course of action could include the development of a toolkit including a taxonomy of terms and conceptual clarity. It was also suggested that DEF should establish a position on data collection.

Building on the importance of collaboration stressed on the Wednesday, it was noted that DEF should develop alliances with similar actors operating in the digital field, collaborating with those who share similar research agendas.

The suggestion to establish a basic quality of digital life standard index and publish an annual barometer report was also offered. Along with this was the idea of developing critical transparency and risk management reports that explore the ways in which transparency is instrumentalised and put to use.

2. Education and Skills

Chair: Anni Rowland Campbell; Rapporteur: Kenny Doyle.

The workshop began by asking what "skills" might be required in the future "digital" world and came up with the following list:

- Digital Media skills including Programming Skills (applications, marketing/communications)
- Data Science (mathematics, computational thinking, code vs computer science)
- "Flip learning" – (http://en.wikipedia.org/wiki/Flipped_classroom) - Experiential learning and student-centred learning
- Self-learning – LEARNING HOW TO LEARN, a recognition of "learning styles", demographic differences, values, capabilities/attitudes/consciousness, diversity, aptitudes and preferences

- Technical skills linked to social skills (Web Science)

It was agreed that “digital” is as much as anything a “way of thinking” which involves an awareness about self and the environment within which we live.

To a very large degree the entire educational system, that has been based on the “traditional” ways of learning now has to be rethought taking into account the needs of the learner within a digitally mediated environment – resulting in people who are “digitally savvy” and who have the skills to learn, but also how to navigate and negotiate in the digital world.

“Digital” is also as much about “experience” as it is about teaching – more so in fact. It is like many of the “trades” in that learning happens by doing, and perhaps we need a kind of “digital carpentry” – an approach where people learn on the job, learn to fix things and learn how things work.

The other thing to recognise is that we live in a physical world, and therefore it is crucial to recognise the inter-relationships between the digital and the physical worlds, something which will become ever more necessary as the “internet-of-everything” evolves. There are many skills and aptitudes from the physical world that we want to make sure we don’t lose – “just because it’s digital doesn’t mean we have to use it.”

We need to build a “skills collateral” – making sure we have people who have a range of necessary but complementary skills. It is not about building a generation of “coders”.

Also, we shouldn’t re-invent the wheel, but we should recognise that where training is happening (i.e. through the major tech companies) there is always an agenda behind that training.

- Time is of the essence, technology moves fast so planning ahead is difficult.
- Governments respond but never lead but some, such as Finland, are beginning to show the way.

3. Digital Ethics

Chair: Michel Riguidel; Rapporteurs: Paula Alaman, Robin Wilton, Jacques Bus

In first instance the discussion focussed on the concepts: what are ethical actors; what do we mean with digital (or maybe better “Informational”?) ethics; what are the principles of ethical behaviour, and how could this govern our digital behaviour.
What do we see as the ethical actors (subjects and objects of ethical acting). Up to now ethics has been mostly about people being the actors as well as the subjects (patients). This seems to be

changing. Autonomous intelligent systems, or algorithms, might act with ethical consequences for individuals, as do organisations. What are the consequences for ethical accountability and responsibility? There is knowledge already developed on distributed ethics in organisations from which one could learn how to deal with the responsibility in a chain of actors.

As shown in the keynote of Peter Paul Verbeek it creates a false opposition to see humans, but not technology, as ethical actors. Humans are mediated by technology. Both are part of the chain of acting and influence each other. Stating that consciousness is needed for ethical acts and hence machines cannot act ethically would support such a false dichotomy. We need a more inclusive argumentation on ethical responsibility and accountability. Given the global Internet and communications we could ask the question whether a universally applicable ethical basis (ontology) can be found that can be taken as a standard.

It seems necessary to implement formal models of digital ethics. A model may for example consist of subjects or ethical actors (individuals, organizations, robots) which enforce an "ethical conscience" (knowledge and behavior) defined by a set of principles that are defined as rules of conduct. If these subjects are robots or systems, their software is governed by principles similar to Isaac Asimov’s axioms for robots. They have at their disposal digital instruments which are used and declared ethical on the environment. These actions, carried out with these tools, produce results that will be declared "ethical" on the environment. Hypothetically, we will consider that the digital ecosystem maintains its ethics and reacts on unethical intrusions.

To start the thinking on the “rules of ethical conduct”, one could take as an example the development of the OECD privacy recommendations which are after 20 years pretty well accepted globally and form a basis for Privacy by Design and Privacy Impact Assessments..Note however that this is not to suggest that ethical behaviour can be fully defined and technically implemented. Ethics is dynamic with society and context dependent. It is normative depending on the culture and community one lives in.

At this moment there is a feeling of ethical dilution, due to the complexity of the action chain involving i.a. humans, systems, organisations. This causes a chaotic situation and a tendency to shift responsibility away. Is technology bringing us closer to or further away from understanding the consequences of our decisions and actions? What is the role of agency? Is complexity not a prerequisite for agency/autonomy? And how does the social innovation that comes with it affect our ethics?

Some specific topics were discussed: Health, Digital Divide, Generational shift, Anonymity.

Elements for actions proposed:

1. Base any thinking of digital ethics on a broad spectrum of ethical actors, including humans, systems and organisations.
2. Do not create an opposition between humans and technology but consider that humans are mediated by technology and vice-versa.
3. Help to bridge the gap between SSH and Technology (tools, translations, conceptual frameworks). Re-align University “silos” for computing and information management. Build genuine inter-disciplinary understanding. Ensure cooperation Tech, Policy, regulation, education.
4. Draft an Ethical Framework not on specific ethical rules, but that is procedural, aiming at facilitating and stimulating ethical behaviour. This should be discussed with all stakeholders and be a starting point to make progress. This Framework could be similar to the set of rules that was developed by the OECD for Privacy.
5. Use the Ethical Framework to start developing infrastructure, methods (comparable to the concept of Privacy by Design) and tools to support the design and development of systems that comply with the framework. Develop tools for individuals and organisation to support them in their ethical behaviour.
6. Humanize systems (checks and balances, system free spaces)
7. Build Trust Platforms that process transactions in an agreed, transparent and auditable way, applicable for specific communities (large or small). This might mimic societal structures of trust.
8. Investigate the idea of “code is law”, taking account of the dynamicity and culture/context dependence of law.
9. Ensure education and give attention to scalability.
10. Stimulate research on non-crypto techniques for information hiding.

Although these steps can help rebuilding the trust in our digital future, it will never be able to foresee all that can go wrong or that might have consequences which will be seen as unethical by hindsight. An act is ethically responsible if, with the knowledge available and known, it is the best that can be done taking account of the accepted balance between the individual and the society. The discussion in the breakout session on Privacy by Design was a clear example of this. For inventions of the order of for example 5G global communication systems it will be very difficult to consider the long term ethical consequences, as it was for our current Internet/Web. The same may hold for serendipitous inventions. Technically mediated phenomena are outstripping human ideas of privacy and ethical outcomes. We can only try to mediate these in our ethical world.

Panel discussions

The **Panel on "Future Challenges"** received the first series of Breakout sessions results as input to their discussions. Based on this and preparatory discussions, including those at the DEF Blog the following questions were discussed at the Panel.

Freedom of will and freedom from discrimination by government or business. What about digital haves and have nots; freedom to experiment and concepts of 'forgive and forget'. Should a commercial (and so commercially driven) algorithm be able to decide what is forgotten and what is remembered? What is acceptable hidden manipulation or discrimination? How can we contribute to a legal and technical infrastructure that includes essential ethical principles, and what should those essential ethical principles be?

Concerning surveillance – by government or business, number of issues were raised:

- what are the policy and technological implications of the future continuation of the climate of fear and insecurity (national, global) that has promoted a variety of surveillance practices and technologies as instruments of (national, international) security and (personal, community) safety?
- how can fair decisions be made on what is 'necessary' and 'proportionate' in society
- what are the prospects for global regulation of surveillance?
- (how) can the transparency and accountability of users of digital technologies by improved?
- (how) can we reconceptualise 'privacy' and 'security' in order to avoid the spurious dualism in the future?
- (why) are we fated to think of privacy as only an individual value or right, and what are the consequences of this for future policies to regulate the effects of surveillance and to combat discriminatory uses of digital technologies?

It was thought that the power of government and business is running away from the rest of us in a most insidious way, including methods of surveillance and policing, although there were not many suggestions about what to do about this.

It is important not to get into the trap of: surveillance bad – privacy good. We need to think how to make this issue politically treatable.

Panel members brought forward the Internet of Things and its potential negative impact on privacy. The opinion was that the impact will be greater than often thought, though there could be an enormous positive economic impact.

Discussion took place on the nature of online secrets (eg Pulcinella; Casanova; King Midas) and the consequences. Are there any real secrets anyway? In fact all information is available some way and the question seems to be “how is it used”. As always: knowledge and transparency need to be balanced by discretion in communities.

Literature and the arts generally are vital to providing us all with an ethical approach to life and to defining the society in which we want to live.

At the end of the panel, it was suggested that DEF might be able to make a contribution in developing:

- A categorisation and listing of technology that has critical effects on privacy, security or trust.
- An ethical framework for the handling of personal information in digital age (possibly limiting it to Big Data).

The **Panel on “The way ahead for the citizen”** received input from the Breakouts on Security and Liberty and Digital Ethics. The following issues discussed were:

The methodology concerning policy-based data to ensure that the processing of data will follow the policies attached to it through metadata. In this context it was suggested that differential privacy could be a way to deal with privacy in Big Data using the policy metadata. Others were critical of the use of differential privacy as it seems quickly to lead to significant loss of relevant information, at least when a reasonable degree of privacy and especially anonymity needs to be achieved by a large-enough anonymity set.

The successful development of the Government Cloud in the UK was presented, with a focus on developing national policies (as for example for the UK) using a web observatory platform to curate a citizen participation and advocacy model.

It was brought forward that there was no clear agreement on the right treatment of personal data in the digital future. In the absence of a shared set of values, the powerful actors – the digital oligarchs and governments – were acting in their own interests and the people appeared to be happy, seduced by the sirens of free services and oppressed by the tyranny of convenience. Reference was made to the 4 levers of control presented by T J McIntyre in his keynote (see above) – the market, norms, architecture and law, and it was suggested that each of these were used by the different actors to meet their own objectives. A personal account of Laurence Millar (see DEF blog) suggests that transparency ("what has happened to my personal data") should be embedded in the architecture of the Internet. It would be difficult for people to recapture control from the digital oligarchs or the government, based on the low interest shown in the issues of privacy and liberty following revelation of the surveillance by governments and corporations working together.

Emphasis was given to the need of reducing complexity of managing their digital life for citizens. While respecting European values in digital life implies a need for citizens to keep (or retain) control over their data, it can turn into the opposite if citizens are overwhelmed by information as well as requests for making decisions. For instance, if executing control over consumer profiling requires making a decision each time you put an item in your shopping cart, there is a risk that many would waive their control and leave it to the service provider to decide what they'd consider best for them. Key factors for reducing complexity include usability (in particular, control mechanisms that do not require technical understanding) and security/privacy by design technologies, for instance, data-driven policies and differential privacy.

The Panel Chair concluded that the way ahead for the citizen in the digital world is not the easy route. However in the struggle for enlightenment routes have never been easy, and this is why DEF exists.

Various reports from blogs by participants:

Anni Rowland Campbell: Moving towards a "digital enlightenment"

Ajit Jaokar: The Implications of the Code as Law

Robin Wilton: Can a Machine Care about Privacy

The Interview: Malcolm Crompton, former Privacy Commissioner of Australia

Sponsored by:

Fāilte Ireland
National Tourism Development Authority

sfi

Digital Enlightenment Forum 2015 - Programme Committee

Peter F. Brown, Consultant, US

Peter Burgess, Director PRIO, Norway, Prof Vrije Univ Brussels

Jacques Bus, Secretary General DEF, Belgium

Jan Camenisch, Research Director, IBM, Zuerich, Switzerland

Kim Cameron, Distinguished Engineer Microsoft, US

Bernd Carsten Stahl, Director CCSR, Univ De Montfort, Leicester, UK

Sandra Collins, Director Digital Repository Ireland, RIA, Ireland

Stefan Decker, Director, Insight Centre for Data Analytics at NUI Galway, Ireland

Claudia Diaz, KU Leuven, Belgium

Willie Donnelly, Vice President R&I WIT, Ireland

Luciano Floridi, Oxford Internet Institute, Oxford University, UK

Harry Halpin, W3C, IRI, France

Mireille Hildebrandt, Radboud University Nijmegen, Netherlands

Peter Hustinx, European Data Protection Commissioner, Brussels, Belgium

Willem Jonker, CEO ICT Labs, European Institute for Technology

Ronald Leenes, Director TILT, Tilburg University

Volkmar Lotz, Director Security Research SAP, France

Sadhbh McCarthy, Director, CIES, Ireland

Kieron O'Hara, University of Southampton, UK

Reinhard Posch, CIO Austria, Univ Graz, Austria

Michel Riguidel, Prof Paris Tech University, Paris, Fance

Wouter Van Wijk, Senior Public Affairs Manager Huawei, Belgium