The IsITethical? Exchange Responsible Research and Innovation for Disaster Risk Management

Monika Büscher, Catherine Easton, Charalampia Kerasidou
Faculty of Social Sciences, Lancaster University
{m.buscher, c.easton, x.kerasidou}@lancaster.ac.uk

Maria Aléjandra Lujan Escalante, Hayley Alter
ImaginationLancaster, Lancaster University
{m.lujanescalante, h.alter}@lancaster.ac.uk

Katrina Petersen
Trilateral,
katrina.petersen@trilateralresearch.com

Marie-Christine Bonnamour, David Lund
Public Safety Communications Europe
{mc.bonnamour, david.lund}@psc-europe.eu

Andreas Baur, Regina Ammicht Quinn, Jessica Heesen
IZEW, Eberhard Karls Universität Tübingen
{a.baur, regina.ammicht-quinn, jessica.heesen}@uni-tuebingen.de

Lina Jasmontaite, Gloria González Fuster
Faculty of Law, Vrije Universiteit Brussels
{lina.jasmontaite, Gloria.Gonzalez.Fuster}@vub.ac.be

Alexander Boden, Britta Hofmann
Usability and User Experience, Fraunhofer FIT
{alexander.boden,britta.hofmann}@fit.fraunhofer.de

Anna Stachowicz, Michał Choraś, Rafal Kozik
ITTI Sp. z o.o. and UTP Bydgoszcz, Poland
{anna.stachowicz, mchoras, rkozik}@itti.com.pl

Kees Boersma
Faculty of Social Sciences, Vrije Universiteit Amsterdam, f.k.boersma@vu.nl

Martina Comes
Faculty of Technology, Policy and Management, TU Delft, t.comes@tudelft.nl

Gemma Galdon Clavell
Eticas Research & Consulting
gemma@eticasconsulting.com

Nicole Föger
Austrian Agency for Research Integrity
Nicole.Foeger@oeawi.at

ABSTRACT

This paper describes the *IsITethical? Exchange*, a European knowledge and service hub we are developing with and for diverse parties involved in crisis and disaster risk management. Their commitment to European values and fundamental rights underpins the rationale of the initiative, which is to support European societies' need for high quality innovation to balance the benefits of IT with fundamental human rights and values, especially privacy and data protection. The initiative is led by researchers at Lancaster University and builds on many years of collaborative design research with a wide range of international practitioners, academics, and commercial IT designers.

Keywords

IT-Ethics; ethical, legal, and social issues (ELSI); disaster risk management, service design, human rights

INTRODUCTION

Societies worldwide are at a crossroads. To realise the potential of Information and Communication Technologies (IT) effectively and responsibly, we must design, use, and govern IT research and innovation with more respect for human rights. Otherwise, human values that are central to human flourishing will be hollowed out, and disenchantment with IT will spread (Wu 2016). In the European Union, fundamental rights regarding the protection of personal data, non-discrimination, and the presumption of innocence underpin values of dignity, freedom, democracy, equality, the rule of law and respect for human rights. People's abilities to enact these rights and values are recognised as critical for peace and justice in Europe and beyond.

Within the European Union, a strong commitment to these rights and values defines policy. European citizens are, for example, 'reassured by developments such as the 'Safe Harbour' decision of the European Court of Justice, [and] the EU is becoming a magnet for digital rights activists and initiatives in search of legal and political openings for challenging uncontrollable mass surveillance and vindicating human rights in cyberspace' (Kaldor, 2016). There is a move towards recognising respect for fundamental rights in IT research and innovation as a key component of high quality innovation and 'human security' policies, which combine a global perspective and a focus on 'prevention, early warning, crisis response and reconstruction as intertwined' (Kaldor 2016). For example, the *Comprehensive Assessment of EU Security Policy* (EC, 2017b), explicitly expresses the European Union's commitment to fundamental rights. Yet, it is extremely difficult to translate such commitments into action, because current forms of IT design, use, and governance do not adequately support people's abilities and practices of enacting or safeguarding fundamental rights and values.

The *IsITethical? Exchange* takes action to support these abilities and practices. It is an initiative led by an interdisciplinary group of scholars at Lancaster University in collaboration with a growing group of international researchers, practitioners, and technology developers, and the Public Safety Communications Europe Network, a community of practitioners, researchers and commercial developers of IT. This alliance builds on completed and ongoing research, including research undertaken in a range of EU projects (please see www.isITethical.eu and Acknowledgements for details). The *IsITEthical? Exchange* combines an online community knowledge exchange platform with a table-top exercise in the form of a board game, services for Responsible Research and Innovation (RRI), and Continued Professional Development.

In this paper, we discuss the background to this initiative, explain the focus on crisis and disaster risk management, and briefly describe the *IsITethical? Exchange* components. We conclude with a discussion of the socio-economic value and future direction of this research, and a brief summary.

BACKGROUND

Increasing numbers of people live in e-societies where 'more information is gathered, collected, sorted and stored about the everyday activities of more people in the world than at any other time in human history' (Andrejevic, 2012: 91). This cuts across a range of different sectors (Figure 1).

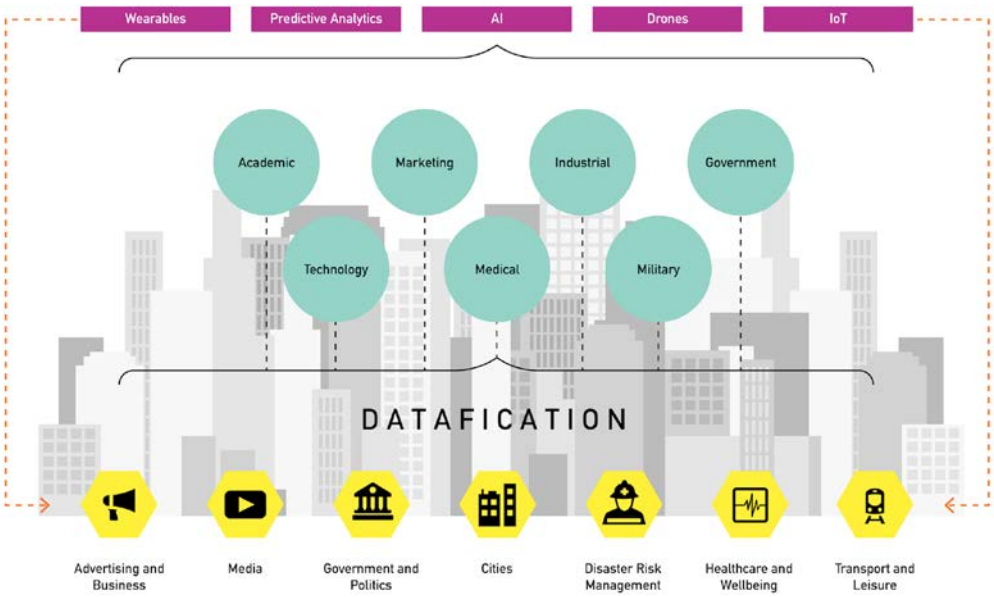

Figure 1 Motivation for building the *IsITethical? Exchange*

To leverage the positive potential of this 'datafication' (Van Dijck, 2014) for comfort, health, jobs and growth, and security, it often seems inevitable that 'trade-offs' against fundamental values, rights and freedoms are made. As datafication cuts across different sectors of society (from advertising to transport and leisure), technologies (from wearables to social media), and arenas of research and innovation (from academia to medical, policy and social innovation), the effects of trade-offs can cascade and magnify.

For example, data produced as a by-product of everyday life could be life-saving in a disaster situation. The city of Amsterdam has been experimenting with techniques to track people's mobile phones within the impact area of a chemical accident (Steenbruggen et al. 2013), and there are now many such contextual sensing and 'Internet of Things' innovations to better detect crises, to dynamically target warnings to mobile populations, and enable faster and more effective evacuation (Dlodlo, 2016). However, such sharing of data in exceptional circumstances also raises complex ethical tensions.

Some examples drawn from the intersection of everyday consumption, political engagement, and security policy will explain key motivations for our *IsITethical? Exchange* concept:

Consumption: Experian's Mosaic synthesizes over '850 million pieces of information to create an easy to understand segmentation of the UK consumer market that allocates 49 million individuals … into 66 detailed Types' (www.experian.co.uk, Lanchester, 2017). Experian is one of Facebook's third-party data partners, enabling Facebook to incorporate offline activities in its analysis of its users' behaviour. Advertisers can thereby target consumers with ever greater precision and even secure 'trusted referrals', the holy grail of advertising (Taplin, 2017). Facebook's Safety Check App tracks its users (and their friends' and families') involvement in disasters, capturing information at a highly emotional and vulnerable time. No data protection regulations are being broken (cf CJEU, 2015), and yet, these activities challenge fundamental rights and values of informational self-determination, and 92% of Europeans are concerned about the use of personal information (Wood and Ball, 2013; 2016 Eurobarometer 443).

Politics: Knowledge production is political. Scientific and commercial research methods of the survey and interview assumed and co-produced the opinionated individual subject of democratic society. New digital capacities to map, track and interrogate people's everyday lives allow governments, the media, businesses, political parties, and the emergency agencies to mobilise forms of population knowledge that constitute a very different 'doing subject' (Ruppert et al, 2013). Knowing this 'doing subject' intimately brings great potential for personalised services, but also means that populism and manipulation can take hold. Political 'hyper targeting' of sections of the electorate can undermine democracy (Grayling, 2017), and established models of public protection. For example, *Cambridge Analytica*, a UK based company that 'uses data to change audience behaviour' has used Facebook 'Likes' for psychosocial profiling to influence elections in the US and Kenya, as well as the UK Brexit referendum (Bright, 2017). Disaster risk management is affected by such practices, because it depends on democratic mediation and public trust. Recent violent attacks against French emergency responders, and the withdrawal of support from humanitarian agencies following news about misconduct attest to the power of mediation, and sensationalist or simplistic media reporting can also fuel a culture of fear focused on terrorism that detracts attention from other dangers, such as extreme weather.

Security: A perceived increase in terrorist attacks underscores a focus on IT as a core part of counter-terrorism strategies, and this has engendered serious controversies. European citizens and civil society organisations are concerned about intelligence and law enforcement agencies, encryption, passenger name records (PNR) (FRA, 2017), and facial recognition in public spaces (Hill, 2017). While fundamental rights are a core concern in EU security policy (EC, 2017b), such concerns are difficult to translate into responsible innovation that respects these rights. In a recent meeting of the high-level expert group on information systems and interoperability for security, the European Data Protection Supervisor found, for example, that he was 'not in a position to endorse all the conclusions' reached by the group (EC, 2017a). He especially raised concerns about the intention to create a common (centralised) identity repository and to 'flag' individuals across different systems, due to 'serious issues in terms of data protection', and concerns about 'purpose limitation and access rights'; elaborating that 'the existence or lack of flag(s) constitutes as such personal data since it contains already some information about an identifiable person (e.g. the person is subject to an alert in the Schengen Information System' (EC 2017a:50) (Figure 2).

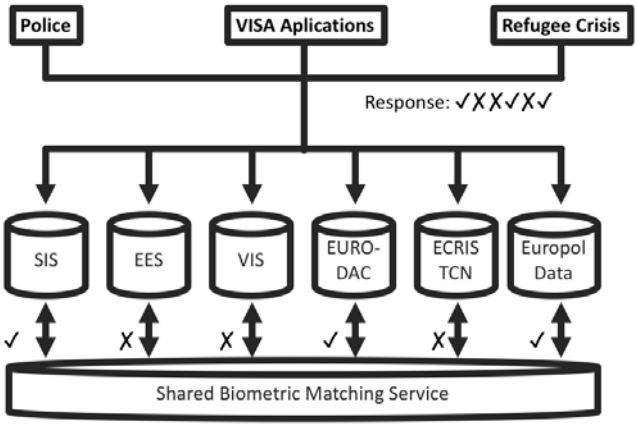

Figure 2 Shared biometric matching service with "hit flags" as discussed in EC 2017a: 31.

These debates highlight how difficult it is to translate respect for human rights into responsible innovation in interoperability and collaborative information management. Many other domains of society, including health, transport, work, and leisure intersect with disaster risk management in ways that exacerbate these challenges. The exceptional circumstances of emergency situations may require that exceptions are made, but they also demand exceptional care lest such exceptions damage important fundamental rights and principles. Crisis and disaster risk management is a domain where ethical tensions arise in particularly significant ways. Most prominent issues are inadequacies of IT design, use, and governance in relation to purpose-binding, informed consent, profiling, surveillance, interoperabilities, and common data repositories. Data breaches and cyber security also pose critical problems, especially around mission critical communications and critical infrastructure.

The *IsITethical? Exchange* addresses these issues, including one of the most significant governance issues: the disparate nature of the legal bases of different information systems. Established EU systems, such as the Prüm System for automated exchange of DNA profiles, fingerprint data or vehicle registration data or new systems such as the European Travel Information and Authorisation System (ETIAS) have been emerging over decades under different institutional contexts, for different (and originally clearly defined) purposes, and there are different legal instruments that regulate the processing of data in relation to each information system, which might impose divergent requirements, notably for the further processing of data. This means that sometimes it is much easier to make something 'technically interoperable' than 'legally compatible' (EGE 2014). Yet, while the diversity of legal bases brings some potentially inconvenient uncertainties, it also creates useful safeguards, as divergences and incompatibilities might be in place for good reasons. Similarly, it is easier to make things technically interoperable than organisationally and culturally shared.

IT research methodologies and innovation also engender new epistemologies that move away from a focus on causation, towards relying on data analytics that highlight patterns (Kitchin, 2014). They are assumed to have the ability to yield new forms of knowledge – embedded in the notion that data is objective and anonymous, and that the more data you collect, the closer you get to the truth. This 'dataism' (Van Dijck, 2014) can not only be difficult to understand and thus make the bases for decisions opaque, it can also introduce machinic forms of reasoning into human affairs in ways that are difficult to align with human rights and values.

In the context of these tensions, ideas of trade-off are coming under attack. Alternatives, such as 'positive sum' approaches (Cavoukian 2013) embed fundamental rights 'in' the technology, for example through 'privacy by design'. Ideas of data stewardship are more alert to the socio-technical, transformative nature of ICT research and innovation. They demand that gains must be balanced transparently against losses and risks, based on a deep and broad-based understanding of what is at stake (EGE, 2014:80, British Academy and Royal Society, 2017). Coupled with ongoing risk analysis (Wright, 2011) and careful regulation that re-locates responsibility for data protection mechanisms, these are promising, but difficult to realise responses.

The *IsITethical? Exchange* approach starts from the premise that attention to ELSI is not a constraint on IT innovation, but, on the contrary, the key to creating high quality IT for human flourishing. The initiative asks how more ethically, legally, and socially circumspect and flexible IT research and innovation can be achieved with a view to the 'big picture', and with detailed attention to abilities and practices of balancing the benefits, losses, and risks of IT research and innovation in crisis and disaster risk management.

IT IN CRISES: BROADBAND, NET-CENTRIC NEW PARTNERSHIPS

Crisis and disaster risk management relies on IT, including personal data routinely processed as part of everyday life with mobile digital technologies in 'smart' cities. There are fears of a data deluge and significant investment in IT is underway (Ferrãos and Sallent, 2015; Lund, 2015). In the UK, for example, a £1.2bn budget is allocated for the transition of public safety communication technology to broadband. This is heavily criticised by the UK National Audit Office (2016) due to the lack of maturity of the technology and the risks associated with acceptance of the technology. Many European countries are embarking on a similar transition path. France aims at developing new communication capabilities to safeguard the public during the 2024 Paris Olympic games, and across Europe, there will be total investments in new broadband communication capabilities for public safety likely exceeding €100's billion. In the US, the recently formed First Responder Network Authority FirstNet has a budget of 7bn $ to develop a nation-wide broadband network over 25 years.

Broadband data promises richer awareness of risks, predictive analysis, more agile response capacity for emergency agencies and communities affected by disasters, better coordination in multi-agency operations, new ways to create a common operational picture and share data, more targeted warnings and broader and richer communications with the public. As the complexity and intensity of risks increase in a '21st Century of disasters' (eSCience, 2012) and budgets tighten, IT can bring much needed new efficiencies and efficacies.

But innovation in this domain is transformative. Disaster risk management models are changing from 'authoritative' and publicly funded command and control to 'datafied', and net-centric approaches (Boersma, 2011). This involves increased monitoring and surveillance of people, assets, and environments, as well as increased public scrutiny of emergency agencies, including 'as it happens' commentaries on response operations live on social media. It enables a focus on prevention, as well as dangers of profiling and social sorting; it gives rise to community risk assessment, crisis mapping, self-organised crisis response, and digital humanitarianism, sometimes coming into conflict with formal agencies. New forms of researching disasters are becoming possible, especially with citizen science (Plantin 2011) and social media data (Palen, et al 2010). At the same time, new public-private partnerships, and new collaborations between formal emergency agencies, volunteers and civil society organisations become possible. These forms of social, organisational, and scientific innovation are disruptive, transforming established responsibilities and accountabilities, including responsibilities for data. Complex ethical tensions arise very concretely and urgently at these junctures between IT research, innovation and fundamental human rights.

In the past, billions of Euros and innumerable hours of work have been 'sunk' into failed IT projects in crisis and disaster risk management across the European member states. Examples include the half a billion-pound failure of the UK Firecontrol project (Committee of Public Accounts, 2011; Yeo, 2002). Research ethics and integrity issues arise, such as in the contest around interviewee confidentiality in a Boston College study of IRA terrorism (Palys and Lowman, 2012), undermining trust in, and influence of, research.

METHODOLOGY

IsITethical? takes a design-led service co-creation approach (Büscher et al 2004, Sanders and Stappers 2008) that draws on methodologies from the newly emerging field of social futures research (Urry 2016). This means that we use creative methods, such as value scenarios (Nathan et al et al 2007) and play (Lujan Escalante and Büscher forthcoming, Figure 6) to collect, assess, and validate rich descriptions of ethical tensions. Methods of controversy mapping and public experimentation (Felt et al 2007, Marres 2009) are part of knowledge exchange workshops, as are methods of 'infrastructuring' for debate and contestation of diverse interests (Le Dantec and Di Salvo 2013). These methods allow practitioners and diverse stakeholders to co-produce, and make concrete, knowledge about tensions and regulatory frameworks, articulate and share guidance, principles, innovative responses, protocols, and standards, as well as recommendations for improvements in regulatory frameworks. Methods from service design (Sangiorgi and Prendiville 2017) are used to co-create these resources within the *IsITethical? Exchange* for Responsible IT Research and Innovation in Crisis and Disaster Risk Management. These also include methods (e.g. Ethical Impact Assessment) and facilitation of value sensitive design, and research integrity protocol implementation. *IsITethical?* partner PSCE (Public Safety Communications Europe Network) facilitates a practitioner-led approach.

THE ISITETHICAL? EXCHANGE

At the heart of the *IsITethical? Exchange* is the fact that ethical, legal, and social issues are complex. As the European Group on Ethics in Science and New Technologies concludes in their assessment of privacy by design, 'embedding ethical reflectivity, … inside a technology … [risks] neutralization of all individuals' ethical potency' (EGE, 2014:80). In other words, 'simplification of issues and solutions, populism and disregard for

evidence in decision-making' are unacceptable (Juncker, cited in FRA 2017:157). The *IsITethical? Exchange* seeks to frame meaningful questions about ethical tensions, and to build evidence-based capacity for reflective practice in the design, use, and governance of IT research and innovation (Figure 3).

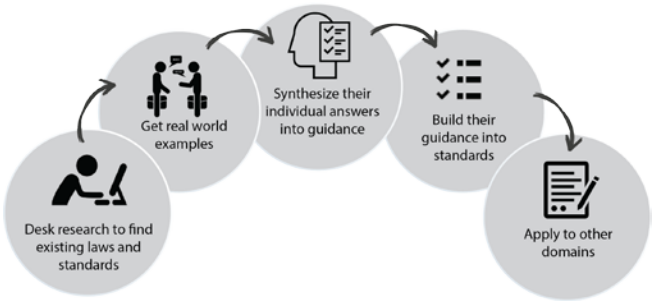

Figure 3 IsITethical? Building guidance for responsible IT research and innovation

The *IsITethical?* knowledge exchange platform curates knowledge about existing and emerging ethical tensions, regulatory frameworks, and responses in an open transnational knowledge base. Its digital and material components and services facilitate broad-based dialogue and make knowledge actionable through examples of innovative pro-active practice, technological design, and regulatory responses. We also contribute to processes of standardisation and are exploring avenues for certification for products and services that proactively develop awareness of, and creative response to, ethical, legal and social issues, without allowing those to become ossified (Balmer et al, 2016). The *IsITethical? Exchange* online community platform is available at www.isITethical.eu. It is a living resource, continuously developed in collaboration with its users. It is designed to underpin the development of a more broadly conceived Hub for responsible IT research and innovation.

There are currently over 40 guidance entries on issues such as 'Access and Fairness', 'Codes of Conduct', 'Data Quality', 'Exceptions and Lawful Processing', 'Goal Diversity', or 'Producing Meta-Data', gathered into five chapters (see Figure 4). Associated with the guidance are definitions of 'Key terms', which are cross linked with the guidance (yellow circles in Figure 5). In addition, we have developed novel methodologies to utilise this co-created guidance to enable creative ethical impact assessment as an iterative process alongside socio-technical innovation, improving the quality of technology and the practices they are meant to support. A mobile '*EtiKit*' helps to build awareness of ethical, legal, and social issues, and capacity to address them creatively and proactively, as a form of continued professional development. The *EtiKit* comprises an *IsITethical?* table-top exercise (Figure 6), techniques for working with the online knowledge exchange platform, and creative ethical impact assessment. *IsITethical?* team members can act as Responsible Research and Innovation Advocates to facilitate knowledge exchange, creative ethical and privacy impact assessment, value sensitive design.

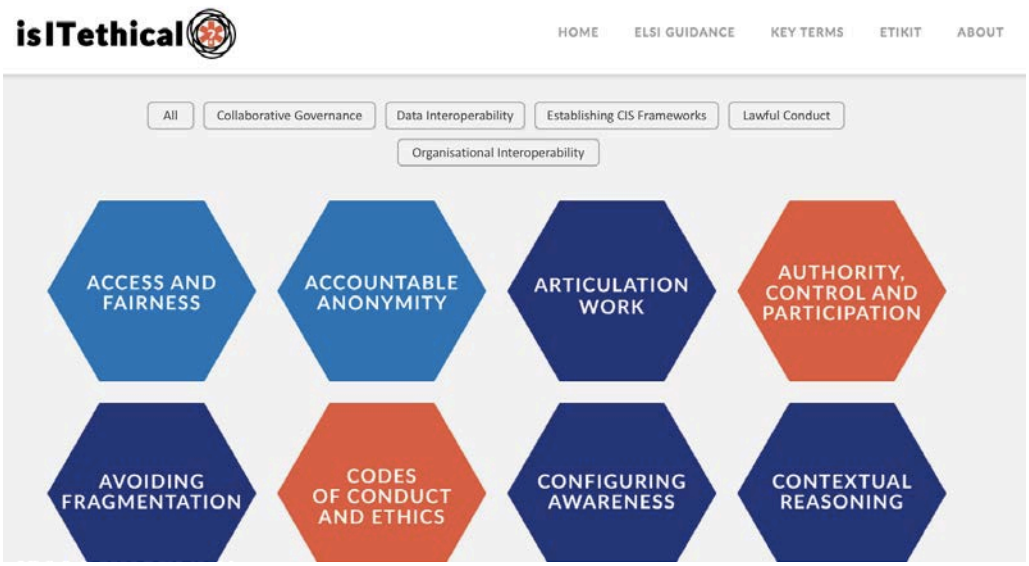

Figure 4 The isITethical? Guidance Overview Page

By inviting participants to discuss examples of how they have encountered and addressed ethical, legal, or social tensions in IT design or implementation, the *IsITethical? Exchange* brings together available knowledge and expertise to take stock of existing, emerging, and future ethical tensions, regulatory frameworks, and responses to develop approaches that place human flourishing at the centre of data governance for the 21st Century. It gathers rich descriptions of tensions and responses to them through real world examples, synthesizes them into guidance that is centred around reflexive questions An excerpt is shown in Figure 5.

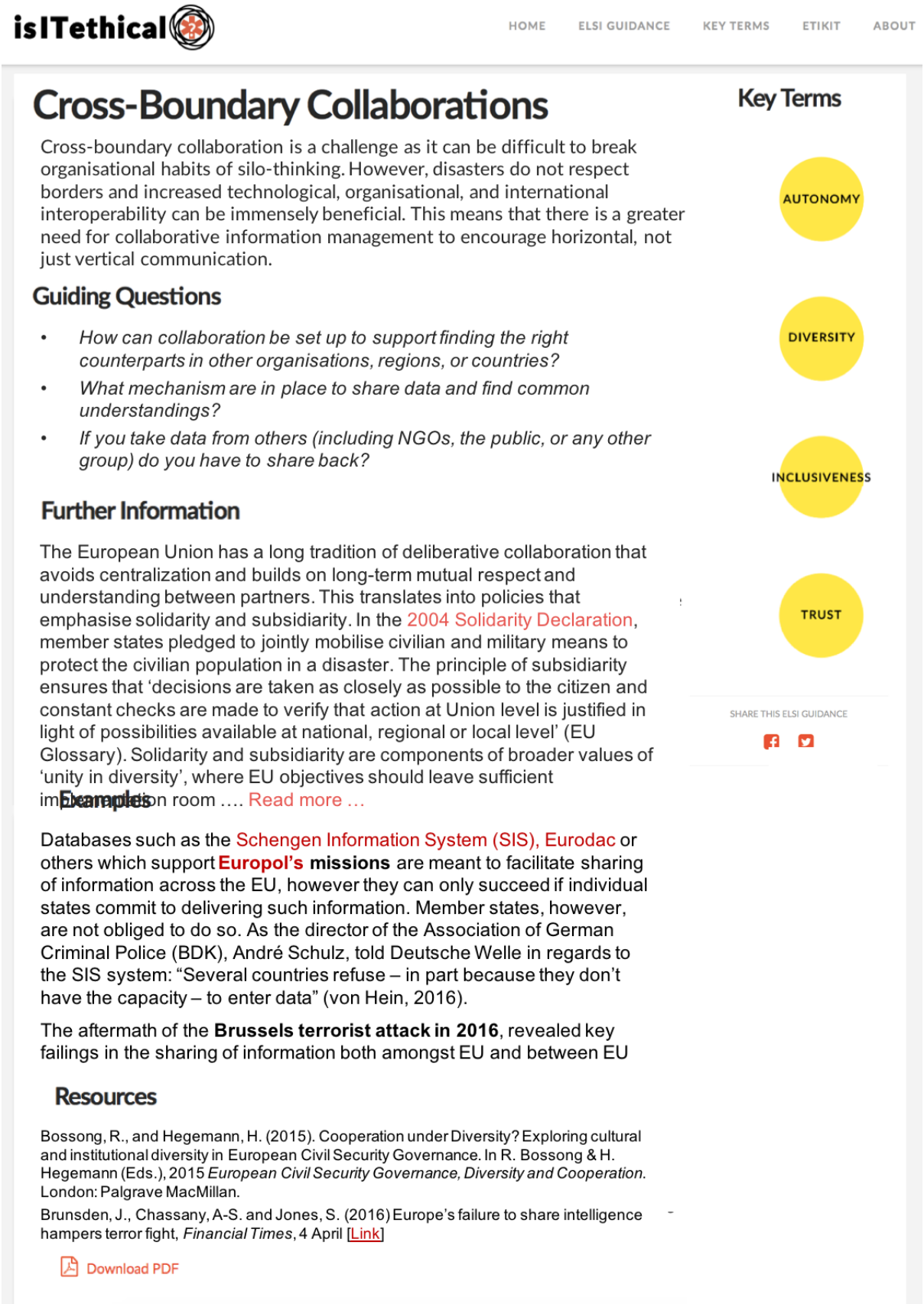

Figure 5 IsITethical? Guidance excerpt.

Building on the knowledge base and guidance on ethical tensions and regulatory frameworks, reflective questions prompt articulation of creative and innovative, proactive responses in IT design and use as well as protocols and standards for responsible research and innovation. The overall aim of the initiative is to build capacity for anticipating, noticing and addressing ethical tensions to facilitate high quality IT research and innovation that goes beyond box ticking and reflexively to pro-actively consider ELSI (Balmer et al, 2016). This is further developed through the *IsITethical? Tabletop Exercise*, which takes the form of a board game that creates opportunities for exchange of expertise and examples, and exploration of the guidance in a collaborative setting, allowing participants to 'step into the shoes' of different roles in disaster risk management (Lujan Escalante and Büscher, forthcoming, Figure 6).

Figure 6 The IsITethical? Table-top Exercise.

The *IsITethical? Exchange* currently focuses on collaborative information management, building on the work of EU projects BRIDGE, SecInCoRe, EPISECC, SECTOR, REDIRNET and ConCORDe, but the initiative builds a broader vision of an open European Hub for Responsible IT Research and Innovation for Crisis and Disaster Risk Management, where services are continuously developed around these resources (including consultancy and facilitation of ethical impact assessment). The initiative recognises the potential and need for engagement with other domains, such as transport, healthcare, e-government, and is developing a framework for this.

SOCIETAL AND SOCIO-ECONOMIC VALUE

Since 2007, 'approximately EUR 980 million have been invested in security research on issues such as CBRN protection (EUR 75 million), explosives (EUR 68 million), critical infrastructures protection (EUR 55 million), intelligence against terrorism (EUR 35 million), preparedness, prevention, mitigation and planning (EUR 150 million), recovery (EUR 17 million), energy, transport and communication grids (EUR 116 million)' (EC 2017b). IT research and innovation that effectively balances security and privacy clearly matters socially, politically, and economically. It is difficult, not just because the issues are complex and contextual.

Traditional modes of public safety communications research and development, and investment are in turmoil. Public safety has conventionally applied monolithic technologies, developed by major industry providers. The combination of specific requirements, limited volume of business and need for significant R&D effort created high entry barriers, and this created specific technological ecosystems operating outside mainstream telecommunication business. All this is changing with broadband, as mainstream standardization (3GPP) and technologies (mobile networks, Apps) are applied and mainstream device ecosystems begin to also address Public Safety (Ferrãos and Sallent 2015). Incorporating attention to balancing the potential of IT with human rights and values early and with awareness for how different sectors are connected can avoid costly failures or retro-fitting.

Moreover, the benefits of Responsible Research and Innovation can help secure maximum benefit of IT potential, address social concerns and achieve good 'alignment' with social values. Responsible research and innovation makes for high quality research and innovation, because it:

> ensures that research and innovation deliver on the promise of smart, inclusive and sustainable solutions to our societal challenges; it engages new perspectives, new innovators and new talent from across our diverse European society, allowing to identify solutions which would otherwise go

> unnoticed; it builds trust between citizens, and public and private institutions in supporting research and innovation; and it reassures society about embracing innovative products and services; it assesses the risks and the way these risks should be managed. (Rome Declaration on RRI, EC, 2014)

IsITethical? supports more transparent, accountable, and inclusive balancing of the benefits, losses and risks of IT research and innovation in relation to fundamental rights and values (Figure 7).

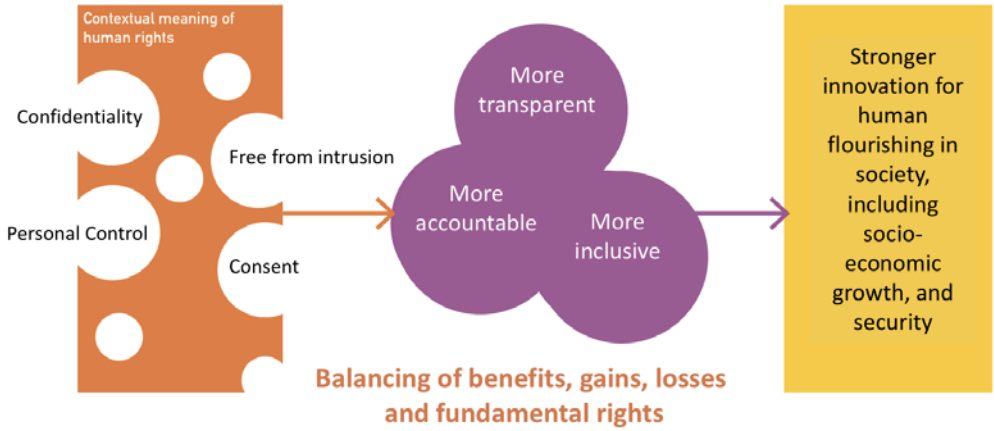

Figure 7 Value added through IsITethical?

It supports stronger, high quality research and innovation for human flourishing, including strong civil liberties, democracy, socio-economic growth and human security. Benefits are not just monetary, but also include making the EU a more attractive environment for a good life, and international investment and innovation.

To sum up, the *IsITethical? Exchange:*

- Brings together a critical mass of stakeholders for practitioner-led co-creation of principles, guidance and standards for responsible IT research and innovation in disaster risk management.
- Creates a space and methodologies for constructive knowledge exchange, critical dialogue around controversies, and articulation of creative and pro-active responses.
- Develops an open knowledge base of existing, emergent, and future ethical tensions in IT research and innovation building out from a concrete focus on the use of common information spaces in crisis and disaster risk management.
- Iteratively co-creates guidance, principles, protocols, and standards through knowledge exchange, where stakeholders evaluate existing guidance, identify gaps, harmonise approaches and bridge differences with reference to concrete examples, technological, social, and regulatory responses and best practice.
- Develops ideas for a European Hub for Responsible IT Research and Innovation that cuts across different sectors.
- Formulates recommendations for improvements of EU Level Regulation.

A CORNERSTONE FOR FUTURE RESPONSIBLE RESEARCH AND Innovation

IsITethical? seeks to accelerate efforts that pursue these aims by building on existing work and the results and networks of the partners in the initiative, including:

- incorporation of ethical, legal and social issues (ELSI) in standard Terminologies for Crisis and Disaster Management (e.g. CEN/WS TER-CDM -2017)
- standards for ethical impact assessment in RRI (e.g. SATORI CEN CWA 17145-2 2017)
- guidance on research integrity (e.g. through the European Network of Research Integrity Offices ENRIO and the European Network of Research Ethics and Research Integrity ENERI)

As part of these plans, *IsITethical?* aims at the institutionalisation of comprehensive guidelines and standards for persons and organisations that are involved in the development and/or application of crisis IT systems, as

well as for the systems themselves. Compliance to these standards could be made visible and accountable by certificates that can be obtained by interested persons and organizations, and that can help to ensure the quality and success of ethically-circumspect technology development projects.

Basis for the certification could be a maturity model in the style of CMMI or Spice (ISO 15504), that would allow to measure the conformity of IT research and development processes to best practices and requirements for ethical IT that are defined in the guidance, the knowledge base that is produced in the project.

For persons, the certificate would confirm that he/she is knowledgeable about the reference process as well as the guidance, and competent in the practice of developing, choosing/deploying and/or using crisis IT systems. For organizations, the certificate would confirm that the organizational procedures and processes implement the requirements of the reference model, which would usually require active involvement of at least one certified employee. For crisis IT systems, the certificate would confirm that the technology has been developed and that it is used within the standards of the reference model, usually requiring the organization to be certified.

In the long-term, certificates could be granted by an independent European certification authority. In order to guarantee the credibility of certificates, accreditation for the certification authority is needed. That ensures that the certification practices are tested and suitable quality assurance processes are employed, e.g. according to ISO/IEC 17024 or related standards.

CONCLUSION

Crises do not respect borders – certainly not in a digital society. Therefore, the aim of improving protection of citizens is intrinsically multi-agency, Pan-European, and global. However, it is often much easier to make things technologically interoperable than legally, socially, and culturally compatible. European values and fundamental rights are immensely valuable to EU (and other!) citizens and highly regarded internationally. The fact that fundamental rights, including privacy and data protection are at the heart of current security policies (EC 2017b) is a case in point. There is a need to expand the role of European approaches in the context of international security policies. E-privacy can be seen as integral, for example, to human security (EGE 2014, Kaldor 2016), and already, the EU is highly attractive for pioneers of high quality innovation in international IT research, technological development and policy innovation. Many who are 'in search of legal and political openings' for alternatives to mass surveillance and datafication (Kaldor 2016), pursue innovation in Europe.

The European Group on Ethics in Science and New Technologies highlights that to achieve better, more transparent, accountable, and inclusive balance and high quality IT research and innovation, it is critical to support 'ethical reflectivity, the perplexity, the pause for thought, the evaluative critical gesture, the valuation and the choosing' that are an essential part of 'all individuals' ethical potency' (EGE 2014:80). *IsITethical?* provides unique leverage by building evidence-based capacity and by connecting organisational, industrial, and research-led innovation through a novel service for responsible research and innovation in disaster risk management. The *IsITethical? Exchange* combines an online knowledge exchange platform with a table-top exercise, and services for creative ethical and privacy impact assessment. This opens up new opportunities for more creative, proactive, and ambitious responsible research and innovation. Making innovation that is not just 'technically interoperable' but also 'legally compatible' and responsible requires finding a balance and 'good' responses to controversies. This is not easy. The *IsITethical? Exchange* enables dialogue between a wide range of parties, who contribute their diverse experiences, interests, and forms of expertise. *IsITethical?* thereby provides guidance that is 'live' in the sense of being available at a click, 'lived' because it is based on practitioners' real world lived experience, and 'living' by virtue of the fact that it engages and involves a diversity of European users, developers, citizens, and researchers to dynamically capture emerging trends.

ACKNOWLEDGMENTS

The *IsITethical? Exchange* is a highly collaborative initiative. A wide range of people have contributed to the content on the online platform, the development of the concept, or have supported the initiative practically. Apart from the co-authors, these include: Matthias Leese, ETH Zurich; Kristof Huysmans, KU Leuven; Toni Staykova, Cambridge University Hospital, UK; Sarah Becklake, Rachel Oliphant, Michael Liegl; Jens Pottebaum, Christina Schaefer, Paderborn University; Blaž Ivanc, Jozef Stephan Institute, Lubljana; George Mourakis, HW Communications, Lancaster; Hayley Watson, Susan Anson, Trilateral; Marijn Hoijtink, Vrije Universiteit Amsterdam, Netherlands; José María Zavala Pérez, Jordi Torrent, ETICAS Research and Consulting, Spain; Remi Gelmini, Jean de Preter, Public Safety Communications Europe; Jeroen van den Hoeven, TU Delft, Netherlands; Mireille Hildebrandt, Vrije Universiteit Brussels; colleagues in the SecInCoRe, EPISECC, SECTOR, REDIRNET, ConCORDE projects, participants in the 2016 PSCE ELSI Workshop, the Information Infrastructuring Workshop at the 2017 Computer Privacy and Data Protection Conference.

REFERENCES

Andrejevic, M. (2012) Ubiquitous Surveillance. In Ball, K., Haggerty, K. and Lyon, D. (eds.) *Routledge Handbook of Surveillance Studies*, Routledge, London, pp. 91-98.

Balmer, AS., Calvert, J., Marris, C. Molyneux-Hodgson, S., Frow, E., Kearnes, M., Bulpin, K., Mackenzie, A. & Martin, P. (2016) Five rules of thumb for post-ELSI interdisciplinary collaborations, *Journal of Responsible Innovation*, Vol. 3, Issue 1, pp. 73–80.

Bossong, R. (2014) The European Programme for the protection of critical infrastructures – meta-governing a new security problem? *European Security*, 23(2), 2014. pp. 210–226.

Bright, S. (2017) After Trump, "big data" firm Cambridge Analytica is now working in Kenya, BBC News, http://www.bbc.co.uk/news/blogs-trending-40792078 [Accessed 12 January 2018]

British Academy and Royal Society (2017), "Data management and use: Governance in the 21st century" London. https://royalsociety.org/~/media/policy/projects/data-governance/data-management-governance.pdf [Accessed 12 January 2018]

Büscher M., Mogensen P., Agger Eriksen M., Friis Kristensen J. (2004) Ways of Grounding Imagination". *Proceedings of the Participatory Design Conference* (PDC), Toronto, 27-31 July, pp. 193-203.

Cavoukian, A. (2013) Privacy by Design, Office of the Information & Privacy Commissioner of Ontario, Canada. https://www.ipc.on.ca/wp-content/uploads/Resources/PbDReport.pdf [Accessed 12 January 2018]

CEN Draft Workshop Agreement CEN/WS TER-CDM (2016). Terminologies in crisis and disaster management. https://www.cen.eu/News/Workshops/Pages/WS-2017-002.aspx [Accessed 15 June 2017]

Committee of Public Accounts (2011), Public Accounts Committee. The Failure of the FiReControl Project, Fiftieth Report of Session 2010-12, London. https://publications.parliament.uk/pa/cm201012/cmselect/cmpubacc/1397/1397.pdf [Accessed 12 Jan. 2018]

Court of Justice of the European Union [CJEU] (2015). "Schrems v. Data Protection Commissioner-Judgemenet of the Court, (Great Chamber)", Brussels, 2015 https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf [Accessed 12 Jan. 2018]

Dantec, C. A. L., & DiSalvo, C. (2013) Infrastructuring and the formation of publics in participatory design. *Social Studies of Science*, 43(2). pp. 241–264. http://doi.org/10.1177/0306312712471581

Dlodlo, Nomusa, "The Internet Of Things For The Safety And Security Of Smart Cities." May, 2016. https://www.researchgate.net/publication/303813523_THE_INTERNET_OF_THINGS_FOR_THE_SAFETY_AND_SECURITY_OF_SMART_CITIES [Accessed 20 January 2018]

European Commission [EC] (2017a). High-level expert group on Information Systems and Interoperability, Brussels, Final Report. http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435 [Accessed 15 August 2017]

European Commission [EC] (2017b) Comprehensive Assessment of EU Security Policy. http://europa.eu/rapid/press-release_IP-17-2106_en.htm [Accessed 12 January 2018]

European Commission [Eurobarometer] (2016). Eurobarometer on e-Privacy, Brussels, 2016. 12.19, https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy [Accessed 12 January 2018]

eScience, (2012) Earth faces a century of disasters, report warns. http://esciencenews.com/sources/the.guardian.science/2012/04/26/earth.faces.a.century.disasters.report.warns [Accessed 12 June 2017]

European Group on Ethics in Science and New Technologies [EGE] (2014) Ethics of Security and Surveillance Technologies, Brussels. Available at http://ec.europa.eu/archives/bepa/european-group-ethics/docs/publications/ege_opinion_28_ethics_security_surveillance_technologies.pdf [Accessed 12 January 2018]

European Union Agency for Fundamental Rights [FRA] (2017) Fundamental Rights Report- 2107, Vienna, 2017. http://fra.europa.eu/en/publication/2017/fundamental-rights-report-2017 [Accessed 12 January 2018]

Felt, U. & Wynne, B. (2007) Taking European Knowledge Society Seriously: Report of the Expert Group on Science and Governance to the Science, Economy and ... for Research, European Commission. IPOC Italian Paths of Culture. 2008. Retrieved from http://www.amazon.co.uk/Science-Governance-Knowledge-Seriously-Commission/dp/8895145259 [Accessed 12 July 2017]

Ferrãos, R., & Sallent, O. (2015) *Mobile Broadband Communications for Public Safety: The Road Ahead Through LTE Technology*. London: Wiley.

Grayling, AC. (2017) *Democracy and Its Crisis*, Oneworld Publishing, London.

Hill, R. (2017) London cops urged to scrap use of "biased" facial recognition at Notting Hill Carnival", The Register, August 27, 2017. https://www.theregister.co.uk/2017/08/17/concerns_over_facial_recognition_at_notting_hill_carnival/ [Accessed 12 January 2018]

Kaldor, M. et al. (2016) From Hybrid Peace to Human Security: Rethinking EU Strategy towards Conflict. The Berlin Report of the Human Security Study Group. London: London School of Economics and Political Science.

Kitchin, R. (2014) Thinking critically about and researching algorithms, Programmable City Working Paper 5., 2014. http://eprints.maynoothuniversity.ie/5715/1/RK_Thinking-Critically.pdf [Accessed 12 January 2018]

Lanchester, J. (2017) You are the product. *The London Review of Books* August 2017, 3-10.

Lujan Escalante, M.A. and Büscher, M. (forthcoming) Playing with datafication in disaster risk management. Available from m.buscher@lancaster.ac.uk

Lund, D. (2015) European Public-Safety Stakeholders Debate Broadband Challenges, Spectrum at PSCE Forum. Mission Critical Communications. Retrieved from http://www.radioresourcemag.com/Features/FeaturesDetails/FID/624 [Accessed 12 January 2018]

Marres, N. (2009) Green Living Experiments, the Ontological Turn and the Undoability of Involvement, European Journal of Social Theory, 12(1), 2009. pp. 117–133.

Nathan, L. P., Klasnja, P. V, & Friedman, B. (2007) Value scenarios: a technique for envisioning systemic effects of new technologies. *Computers and Society*. ACM. pp. 2585–2590.

Palen, L., Anderson, K. M., Mark, G., Martin, J., Sicker, D., Palmer, M., & Grunwald, D. (2010) A vision for technology-mediated support for public participation & assistance in mass emergencies & disasters. In Proceedings of the 2010 *ACMBCS Visions of Computer Science Conference. British Computer Society. 2010*. pp. 1–12.

Palys, T., & J. Lowman, Defending Research Confidentiality (2012) To the Extent the Law Allows: Lessons From the Boston College Subpoenas. *Journal of Academic Ethics*, 10 (4), pp. 271–297.

Plantin, J.-C. (2011). "The Map is the Debate": Radiation Webmapping and Public Involvement During the Fukushima Issue. In *Proceedings of the A Decade in Internet Time: OII Symposium on the Dynamics of the Internet and Society*. Southampton. http://doi.org/10.2139/ssrn.1926276

Ruppert, E., Law, J. & M. Savage (2013) Reassembling Social Science Methods: The Challenge of Digital Devices. *Theory, Culture & Society*, 30 (4), pp. 22–46.

Sangiorgi, D., and Prendiville, A.(2017) Designing for Service : Key Issues and New Directions. Bloomsbury Publishing PLC.

European Union (EU) Rome Declaration on Responsible Research and Innovation in Europe. 2014 https://ec.europa.eu/digital-single-market/en/news/rome-declaration-responsible-research-and-innovation-europe [Accessed 27 August 2017]

Sanders, E.B., & Stappers, P.J. (2008) Co-creation and the new landscapes of design". *CoDesign*, 4, pp. 5–18.

SATORI CEN Workshop Agreement Ethics assessment for research and innovation - Part 2: Ethical impact assessment framework CEN CWA 17145-2 2017 Workshop Agreement. 2017. http://satoriproject.eu/media/CWA17145-23d2017.pdf [Accessed 27 August 2017]

Steenbruggen, J., Borzacchiello, M. T., Nijkampa, P. and Scholten, H. (2017) Data from Telecommunication Networks for Incident Management: An Exploratory Review on Transport Safety and Security. *Transport Policy*, 28, pp. 86–102.

Taplin, JT. (2017) *Move fast and break things: how Facebook, Google, and Amazon cornered culture and undermined democracy*. Little, Brown and Company Publishing, New York.

UK National Audit Office. Upgrading emergency service communications: the Emergency Services Network. 2016. https://www.nao.org.uk/wp-content/uploads/2016/09/Upgrading-emergency-service-communications-the-Emergency-services-Network.pdf [Accessed 25 July 2017]

Urry, J. (2016). *What is the future?* London: Routledge.

Van Dijck, J. (2014) Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology, *Surveillance & Society*, 12 (2), pp. 197-208.

Wood, D. M., & Ball, K. (2013). Brandscapes of control? Surveillance, marketing and the co-construction of

subjectivity and space in neo-liberal capitalism. *Marketing Theory*, *13*(1), 47–67.

Wright, D. (2011) A framework for the ethical impact assessment of information technology, *Ethics and Information Technology*, 13 (3), pp. 199–226

Wu, T. (2016) *The Attention Merchants*, Alfred A. Knopf-Penguin Random House: Toronto.

Yeo, K. T. (2002) Critical failure factors in information system projects, *International Journal of Project Management*, 20 (3), pp. 241–246.