Information Polity 27 (2022) 121–129
DOI 10.3233/IP-229006
IOS Press

Editorial

Introduction to the Special Issue: *Questioning Modern Surveillance Technologies: Ethical and Legal Challenges of Emerging Information and Communication Technologies*

Johann Čas[a,*], Paul De Hert[b], Maria Grazia Porcedda[c] and Charles D. Raab[d]
[a]*Institute of Technology Assessment, Austrian Academy of Sciences, Vienna, Austria*
[b]*Vrije Universiteit Brussel, Brussel, Belgium*
[c]*School of Law at Trinity College Dublin, Dublin, Ireland*
[d]*Politics and International Relations, School of Social and Political Science, University of Edinburgh, Edinburgh, UK*

1. Overview

Security issues have always been and will always be high on the public policy agenda. Similarly, new technologies, particularly surveillance technologies, are developed and deployed to tackle security problems. Persistent, conventionally perceived security threats such as organised crime, terrorism and public safety, are complemented by new concerns, such as the social and individual effects of technological solutions to manage the threat posed by the COVID-19 pandemic or challenges to democratic processes posed by the use of social media. Information and Communication Technologies (ICTs) often appear to offer simple, technologically based solutions to multidimensional problems relating to the safeguarding of societies, people and nations. This impression is sustained both by the activities of commercial interests, who would like to see the ongoing procurement of security and surveillance technologies, and by the stance of policy-makers, who have to deal seriously with security problems but who also search for symbolic policies and tools as a way of demonstrating proactivity against crime, terrorism and radicalisation. Conversely, technological progress can also be seen as a factor reinforcing existing securitisation trends; emerging security concerns and technical capabilities mutually fortify each other.

*Corresponding author: Johann Čas, Institute of Technology Assessment, Austrian Academy of Sciences, Vienna, Austria. E-mail: Johann.Cas@oeaw.ac.at.

Emerging ICTs form a fundamental component of the new generation of security and surveillance technologies, in that they allow for the collection, analysis and interpretation of large quantities of data, in unprecedented and previously unforeseen ways. In the context of this Special Issue, emergent ICTs relate to a wide range of technological tools and applications that are an amalgamation of enhanced capabilities to generate and process data, including by new sensory devices embedded in the Internet of Things (IoT), and rapid advances in data science that allow for the utilisation of artificial intelligence (AI) for enhanced biometrics, interpretation of emotions and predictive policing, among other purposes.

The digitisation of everyday life is increasingly blurring the boundaries between the use of ICTs to provide everyday services and their use for surveillance and security purposes. The enormous amounts of data generated, accompanied by enhanced analytical capability, create not only a desire to use data for commercial purposes, but also complementary temptations to exploit them in the context of security. Revelations about mass surveillance programmes in a number of countries and the apparent lack of democratic oversight point to the overwhelming temptation to use data in this way, arguably to the detriment of individual autonomy, dignity and human rights in general.

Delivering security in a digitised world is complex, involving traditional and new security concerns, pressure from commercial interests, democratic and political control issues, intricate unaccountable data flows, as well as new digital ethical issues around transparency, accountability, fairness and trust. The pervasiveness of ICTs and the dependence of modern societies on the uninterrupted availability of ICT infrastructures and services have made ICTs themselves a core security concern. This relates to the security of critical infrastructure and cybersecurity in general, as well as the market dominance of a few big commercial interests that – it is argued – threaten the autonomy, liberty and privacy of individuals and the (digital) sovereignty of nations, whatever that may mean.

New ICTs have become deeply engrained in all facets of society, including contemporary democratic and public-policy processes. Public policy is increasingly reliant on core technological platforms and data flows, suggesting a shift in power from political to commercial interests who benefit from the monetisation of data analytics. ICTs can be seen to play a critical role in politics and public policy, for example as tools to influence elections through the distribution of 'fake news' or where governments seek to limit freedom of expression and information by automatic censorship. Moreover, the rise of populist governments and political instability weakens regulatory oversight and opens up spaces for the use of ICT in potentially unethical ways.

This Special Issue explores ethical and legal challenges of existing and emerging ICTs used in the context of security and surveillance from the vantage point of several disciplines and interpretive paradigms. The contributions discuss issues and gaps existing in current regulatory frameworks and planned policy measures designed to address the challenges associated with the promotion of digital technologies in society. They address the need to develop ethically compliant practices and data processes. Individual papers tackle the complex intertwined relations between security, ethics and human rights; the significance of commercial interests in democratic and policy processes; and assessments of innovative new policies or practices, including those that are technology dependent, or those that seek to support human rights, democratic values and societal development. The call for papers in March, 2021 yielded 25 abstracts; 11 articles were selected for publication after the peer review and editorial selection processes.

These published contributions reflect the broad range of aspects addressed in the Call for Papers. Although the boundaries between contributions are fluid, they can be categorised by focus. Regulation is discussed by several authors: thus the articles by Orru, by Gremsl and Hödl, by Nesterova and by Clarke critically discuss mainly ethical and legal aspects of current and forthcoming regulations in the European Union, while De Hert and Bouchagiar analyse the European Union's approach to facial, visual

and biometric surveillance, with a view to submitting a new paradigm for desirable bans on certain intrusive practices. Technological systems in law enforcement are the subject of the contributions by Eneman, Ljungberg, Raviola and Rolandsson and by Pedrozo and Klauser; IoT-derived 'witnessing' in the context of criminal justice is examined by Urquhart, Miranda and Podoletz. Eliot and Murakami Wood change the scene in their investigation of Federated Learning of Cohorts (FloC) in online marketing and user behaviour, while the theoretical and methodological article by Rudschies develops an approach to the analysis of power hierarchies within surveillance constellations. The Special Issue is rounded off with a thought-provoking essay by Gary T. Marx on the information age's 'techno-fallacies'. This Special Issue finishes with the review of Bryce Clayton Newell's book "Police Visibility: Privacy, Surveillance, and the False Promise of Body-Worn Cameras" (2021) conducted by Diana Miranda.

2. Introducing the articles

The sense of insecurity caused by terrorist attacks on European soil influenced the EU political climate and permitted the adoption of the EU Passenger Name Record (PNR) Directive in 2016. The PNR is a system that exploits data produced while booking a flight with the purpose of investigating and prosecuting serious crimes and terrorism. This Directive was innovative since it introduced a pre-emptive approach to intra-European information exchange, obliging all EU member states to adopt the necessary legislative acts and measures to make it applicable.

Even though the PNR is deemed to be useful and effective in its purposes, this affirmation is based on the assumption that travel-related information can provide an indication of a potential traveller's plan to engage in some criminal or terrorist activity. This assumption raises a series of topics that are primarily addressed by Elisa Orru's article, "The European PNR Directive as an instance of pre-emptive, risk-based algorithmic security and its implications for the regulatory framework" in contemplating the implications of the Directive. Firstly, the pre-emptive model rejects the option of eliminating crime by addressing its causes. Instead, it deems non-prohibited behaviour to be high-risk, based solely on the empirical data. Additionally, it leans completely on non-verified data that is highly susceptible to illogical circumstances to predict a hypothetical future whose realisation is not verifiable. This opaque security system poses both a challenge and a problem to the rule of law at the same time as it shifts the relationship between the ruled and the rulers, heavily influencing how individuals address the norms and how these norms are conceived. Using a critical-realistic approach, Orru analyses the measures and practices introduced by the EU PNR, pointing out how pre-emptive, risk-based security measures can barely be reconciled with the principles of legal certainty and human autonomy; she suggests possible remedies to illuminate the tensions and contradictions caused by the Directive.

The application of AI-based surveillance technologies has raised major concerns about their impact on fundamental rights, the rule of law and democracy. To address these concerns, the European Commission published in 2021 its proposal for an AI Act that would create the first legal framework laying down harmonised rules for the deployment of AI technology in the EU. In her article, "Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance", Irena Nesterova analyses the extent to which the proposal succeeds in addressing risks posed by AI biometric surveillance systems.

The author acknowledges that the introduction of prohibitions on certain AI practices contradicting EU values and fundamental rights would constitute a significant step forward in debates that have taken place at the national, European and international level. However, she identifies shortcomings in the proposal with regard to biometric surveillance techniques that would risk undermining its efficiency and

the achievement of its purported objectives. The current classification of several biometric surveillance methods as 'high risk' or 'limited-risk' AI systems would not sufficiently safeguard against fundamental rights violations. The use of remote biometric identification systems, for instance, could almost always be justified for law enforcement purposes. Furthermore, a lack of precision in the wording on conditions for justified uses would risk normalising or even legitimising their deployment. The proposal of the AI Act would therefore not prevent the use of AI systems for mass surveillance purposes. Only a general ban on, for instance, emotional recognition systems or the use of AI for automated recognition of human features in publicly accessible spaces would provide for sufficient safeguards.

The author therefore calls on EU legislators to take "courageous further steps" and to draw additional red lines in cases of biometric surveillance. Such measures should go hand in hand with strengthened transparency and accountability requirements by introducing, for instance, impact assessments that would require users of high-risk AI systems to appraise to what extent fundamental rights, democratic values and the rule of law are impacted. Together with an enhancement of existing data protection standards and the introduction of legal remedies for individuals in cases of human rights violations, the AI Act proposal should be turned into a tool that addresses in a more meaningful way the risks AI poses to our society.

Thomas Gremsl and Elisabeth Hödl's article, "Emotional AI: Legal and ethical challenges" takes stock of the legal and ethical implications of AI-based human emotion recognition systems (AI ERS) considered by the European Commission's proposed AI Act. The authors stress that the proposed definition of emotion recognition systems fails to define emotions and emotional data, which can be personal and even biometric data, thus attracting the protection of EU data protection law. However, the right to personal data protection is only one among the many rights enshrined in the Charter of Fundamental Rights and the European Convention on Human Rights that could be undermined by AI ERS; other rights include dignity and freedom of thought, which includes the freedom to keep one's thoughts secret. The article questions whether the proposed AI Act's lofty goal of safeguarding fundamental rights is matched by adequate protections, as exemplified by provisions on transparency and exemptions for law enforcement authorities.

An area of ethical concern rests in the combination of AI ERS and social scoring systems used in some countries in pursuit of the 'common good' of which, however, there are different conceptions. Although the AI proposal bans such scoring systems on account of the unacceptable risks they pose to people's livelihood, the article identifies three human-centred traditions predicated on human dignity that help to outline the ethical boundaries for AI ERS. Thus, AI ERSs would be ethical if they respected the common good understood as social peace and distributive justice (Catholic social teaching), saw humans as the end-goal, rather than an instrument for collecting data points (Kant), and if they did not deny individual autonomy and subjectivity (Nussbaum). In essence, Gremsl and Hödl stress that AI ERS should be developed with people's well-being in mind.

Roger Clarke's paper, "Responsible Application of Artificial Intelligence to Surveillance: What prospects?" looks at the prospects for the responsible use of artificial intelligence in surveillance. It begins with a brief history of AI, which was marked by a series of exaggerated expectations that did not materialise. Claims about the successful use of AI still need to be proven, especially in the context of surveillance, due to lack of publicly available evidence. The observed obfuscation is compensated for by an identification of potential uses of AI technologies based on their general characteristics, i.e., a brief and concise description of approaches and methods grouped under the term AI. In a similarly concise manner, the disadvantages and risks of AI are summarised; a central element here is the decreasing or complete lack of explainability with the increasing complexity of AI procedures, which undermines both accountability and the use of the results in court. Consequently, effective regulation of the use of AI for surveillance purposes is indispensable.

Based on a multi-level hierarchy of regulatory mechanisms, ranging from system-immanent natural regulation to state formal regulation, Clarke analyses the possible contributions of regulatory approaches on the different levels as well as of further instruments such as impact assessment, the precautionary principle or ethically based principles. Due to the low probability that combinations at the lower levels can effectively counteract the major threats posed by AI, the possibilities of formal regulation are discussed in more detail on the basis of the draft AI Act. This draft distinguishes four levels of risk: unacceptable, high risk, limited and minimal. Only a few AI practices would be prohibited; high-risk applications would be subject to a number of safeguards; certain transparency requirements are foreseen for the next category; and the rest would not be affected. The draft AI Act is assessed against 50 Principles; compared to the EC's High-Level Expert Group on Artificial Intelligence's Trustworthy AI Guidelines, the current draft scores much lower. The author's sobering conclusion is that the current draft is not a serious attempt to protect the public in general and with regard to surveillance applications; too much preference is given to economic interests.

De Hert and Bouchagiar's article "Visual and biometric surveillance in the EU: Saying 'no' to mass surveillance practices?" analyses the European Union's approach to facial, visual and biometric surveillance, with the objective of submitting some ideas that the European legislator could consider when strictly regulating such practices. More concretely, with the European Citizens' 'Civil society initiative for a ban on biometric mass surveillance practices', already registered by the European Commission, citizens are given the opportunity to authorise the Commission to suggest the adoption of legislative instruments to permanently ban biometric mass surveillance practices. The article finds the above initiative particularly promising, as part of a new development of bans in the European Union.

The authors address the European Union's legal regime, as framed under the General Data Protection Regulation (GDPR) and the Data Protection Directive for Law Enforcement and Criminal Justice Authorities. Their overarching narrative is that the European Union has failed to say a clear 'no' to certain surveillance practices that may have a particularly hostile impact on fundamental human rights and freedoms. They argue that some banning techniques could assist the European legislator in introducing bright-line prohibitions on certain technological uses. In their article, they submit a new paradigm for introducing desirable bans: first, the EU privacy/data protection framework, currently permissive, could become honestly prohibitive regarding technologies whose use may be particularly harmful or dangerous; second, certain techniques, like moratoria prohibiting certain technological uses until proven safe, could be adopted at the European Union level; and, third, the European Union's approach to data protection, currently highly process- and procedure-based, could combine different elements known from other fields (like criminal law or the market sector) that can make applicable rules more comprehensively applied.

Marie Eneman, Jan Ljungberg, Elena Raviola and Bertil Rolandsson address the application of AI-based facial recognition by police authorities in their paper, "The Sensitive Nature of Facial Recognition: Tensions between the Swedish police and regulatory authorities". They examine how the deployment of facial recognition technologies is influenced by the interplay of regulatory requirements and the mandate to use technological capabilities in policing, and how the trade-off between security and privacy unfolds in a concrete example. The research design and empirical analysis relates to an unauthorised use of Clearview AI facial recognition services by Swedish police authorities, which was sanctioned by the Swedish Data Protection Authority with a fine of approximately €250,000. For this purpose, publicly available documents from three authorities were reviewed, the Data Protection Authority, the Police Authority and the Administrative Court.

The evaluation is oriented towards three main conflicts: effectiveness versus privacy, i.e. balancing the desire for effective investigative tools with the protection of citizens' privacy; organisational responsibility

versus individual professional discretion, i.e., establishing and enforcing rules that provide a binding framework for the use of these technologies; and internal versus external technology, thus addressing the question of the extent to which the services of private companies can be integrated into policing, especially when their business model is considered illegitimate. Although the institutional dialogues between three Swedish authorities are at the centre of the analysis or conclusions, the issues outlined are of a general nature and thus the conflicts identified and their implications are also relevant to the use of facial recognition by investigative authorities in general.

In their article, "Policing the Smart Home: The Internet of Things as 'invisible witnesses"', Lachlan Urquhart, Diana Miranda and Lena Podoletz combine findings from socio-technical and forensic research to discuss the profound implications of the design and application of IoTs for contemporary life and criminal investigations. The in-built invisibility of IoTs hides the trade-off between usability and privacy, thereby depriving users from choosing whether they want to forgo the home as a Goffmanian backstage where they enjoy the intimacy necessary to develop autonomously and flourish. IoTs push the home into a permanent front stage producing longitudinal data on users' once- private behaviour. What is more, some may suffer greater privacy loss as IoTs enable a householder to impose surveillance on unwitting cohabiters.

As private behaviour includes criminal activity, the authors draw from anecdotal evidence to demonstrate how IoT devices leave digital traces with evidentiary value predicated on the ability to point to deviation from 'standard' behaviour. The evidentiary value of IoTs needs to be carefully scrutinised due to their potential for circumvention of well-developed safeguards against disproportionate intrusions into home and family life.

The authors do not scrutinise the legal implications of cross-border access to data held in the clouds, which may anyway vanish as we move towards edge computing. Instead, they focus on the cacophony of 'witness statements' produced by IoT devices undermining the crime narrative and on issues inherent to data extraction and preservation. The authors caution against the ability of IoTs to tell a partial story, link activity on a shared device to the wrong users and reinforce tunnel vision and confirmation bias. The authors also highlight the limitations of data extraction, the exposure of data to cybercrime and tampering (including when IoT devices are in custody) and – in general – the reliability of data, the analysis of which increasingly requires the use of automated tools.

Police forces in many countries have become equipped with unmanned aerial vehicles (UAVs) or 'drones', as important pieces of technology to enhance their capability in detecting crime, finding missing persons, monitoring activities taking place in public spaces, and other activities associated with law-enforcement and the maintenance of public order. The cameras that drones carry provide powerful tools for gathering information and evidence; drones flying overhead have an impact on populations that might experience their physical presence as a means of surveillance – whether ominous or reassuring – in the interests of safety and security. Drones have therefore become controversial and cannot be seen as 'just another technology' for policing. There is a lack of public knowledge about their functions, capabilities and effects, and little transparency about the decisions and processes by which police forces come to adopt them as an important resource.

The latter is the subject of the case-study by Silvana Pedrozo and Francisco Klauser, "Between Formality and Informality: A critical study of the integration of drones within the Neuchâtel Police Force". Their research focuses upon three main aspects of the plans and procurement processes by which Neuchâtel became the first force in French-speaking Switzerland to acquire and integrate drones into their armoury. These are the formal and informal practices involved, the relationship between private and public interests, and practical expertise mediating this development.

Using qualitative empirical evidence, the authors show how informal, curiosity-driven individual initiatives later developed into more formal institutional deliberation and adoption of drones. Concepts of 'institutional bricolage', improvisation and personal networks cast light on stages of this trajectory as relationships were forged that led to further familiarisation with drones, official meetings, reporting, political decisions and budgeting as drones were integrated into police practice. The crucial informal processes and their relationship with formal ones faded from the official report's narrative and were hidden from public view, exacerbating the problem of democratic control that the authors highlight by asking how the increasing digitisation of policing can be made more transparent for public debate.

The paper "Culling the FLoC: market forces, regulatory regimes and Google's (mis)steps on the path away from targeted advertising" by David Eliot and David Murakami Wood analyses a failed attempt to replace the use of third-party cookies in targeted advertising with a privacy-preserving, AI-based process called Federated Learning of Cohorts (FLoC). The concept of FloC is comprehensively described, the privacy expectations attached to it and its weaknesses are explained. The relationship to the GDPR and to planned regulations in the United States is also briefly addressed.

The second main section is devoted to discussing the connection between surveillance capitalism and targeted advertising. Building on a brief outline of the long-standing debate on surveillance, data, corporate form and capitalism, four factors are identified that influence the move away from revenue from targeted advertising towards the development of AI as the main source of future revenue: 1. corporate ideology; 2. market pressures; 3. regulatory regimes, and 4. internal cultural controversies. Corporate ideology refers to Alphabet's long-term goal as an "AI-first" company to create a platform for solving all kinds of challenges, for the future governance of the planet. Market pressures are understood to mean, for example, the need to compensate for the declining importance of advertising revenues by providing even greater access to personal data in order to be able to offer personalised AI services. In the case of regulatory regimes, different regional priorities are addressed, in particular the conflict between the protection of fundamental rights and the maximisation of economic returns. Internal cultural conflicts concern, for example, the relationship to military projects or the development of genuine AI ethics.

Power is a central concept in political science and allied disciplines. It is also a term that is freely used in daily parlance and in the discourse about 'surveillance society' and its technologies, especially when a critical and resistant stance is taken about impacts and effects, disadvantage, injustice, and the political and economic interplay of the haves and have-nots. Defining 'power' and turning it into a researchable concept has always been a focus of academic debate about concepts and methodology, and an elusive pursuit. This is often eschewed in surveillance studies in favour of intuitive, assumptive and less nuanced understandings that can obscure rather than illuminate the processes by which power is acquired and used. Who are 'the powerful' and what gives them 'power' are questions that can give rise to glib and non-empirical answers.

Catherina Rudschies grasps this nettle in her article, 'Power in the Modern "Surveillance Society": From Theory to Methodology', in which she uses a 'meso-level' lens to focus attention, sequentially, on observers and the observed in any surveillance relationship: these are seen as roles that do not define permanent socio-political positions. Looking at resources, motives, and structural positions on the side of the observer, and at the observed's means of avoidance or resistance and the degree of their exposure to observation, she advances several hypotheses or 'indicators' that aim to use these variables to explain the degree of power the two sides have in the surveillance relationship. The analytical framework that she sketches is aimed at getting closer to understanding power, but is proposed as an early ground-breaking step in avoiding a priori judgements. Whether we are brought nearer to an understanding and measurement of power in surveillance, while avoiding circularity and tautology, is an assessment that requires empirical

research as well as 'further development and discussion' in future, in order to assess the validity and usefulness of this approach.

Gary T. Marx's 'Essay on Complex Problems and Simple Solutions: Techno-fallacies in the information age' is the last article of this Special Issue. He takes on the challenge of identifying and demystifying the tropes that inform the relationship between technology and humans in their guise of technophiles, technophobes as well as academics standing in-between. The bulk of the essay is devoted to undoing the – often very simple – arguments of technophiles. Marx discusses 15 fallacies of tech-determinism and scientific technological perfection that underpin the blind faith in technology that animates many entrepreneurs in their pursuit of economic and political interests. Such fallacies contribute to the overlooking of problems that may be created by new technologies, and downplay the crucial role played by humans in making choices infused with value. The author also engages with nine fallacies on values and persons that embody the objectification and manipulation of individuals for the sake of efficiency gains. Those fallacies frame people as objects to be controlled rather than as bearers of dignity.

Marx also reproaches academics for locking themselves up in an echo chamber of technophobia that paints technology as the harbinger of inequality and domination and informs at least eight technophobic fallacies. The essay finishes on a self-deprecating note, where the academic self-reflexively observes the pitfalls of neutrality and objectivity. As the essay invites the reader to enjoy a narrative of the fallacies, this summary will not spoil the pleasure of the discovery. Rather, it invites readers of this Special Issue to observe the many parallels that can be drawn between Marx's essay and the preceding papers in their common attempts to demystify simplistic approaches to technology and the dangerous effacement of values.

Finally, this Special Issue closes with Diana Miranda's very informative book review of *Police Visibility: Privacy, Surveillance, and the False Promise of Body-Worn Cameras*, by Bryce Clayton Newell (2021). His book provides a highly relevant empirical and legal analysis of the introduction of body-worn cameras and their impact on police practice and the privacy of civilians.

3. Conclusion

This Special Issue offers a broad and comprehensive insight into ethical, economic and legal aspects of the use of new ICTs as surveillance tools. Of course, this collection remains necessarily incomplete, especially if one dares to look ahead to future generations of ICTs. The rapid advances in technologies which on the one hand directly or indirectly generate personal data and which on the other hand also allow these immense amounts of data to be searched and analysed, give the impression that the Glass Man has long since become a reality. Nevertheless, technical developments are on the horizon that should enable even deeper, even more comprehensive insights not only into our actions but also into our thinking. It remains to be seen, for example, to what extent future mind-reading technologies will be suitable for concretely penetrating our consciousness. Regardless of the extent to which the high expectations can realistically be fulfilled, the promises alone will provide enough incentive to put these technologies to practical use. But it is not only our inner selves, our freedom of thought, that is threatened.

The environment in which we live is also becoming an open book in hitherto unthinkable ways with the introduction of new generations of mobile networks and radio frequency sensor technologies. Not only do these technologies allow device-free gesture and activity recognition based on micro-Doppler fluctuations, even the smallest movements, such as breathing or pulse, can be analysed to sense our emotions or moods. Future methods of radio frequency holography could also be used to perceive objects or movements in three dimensions, even through walls. This also poses enormous challenges for the future

governance of these technologies to ensure to use them in an ethical and fundamental rights compliant way. These challenges may require both the development of new regulatory instruments and the effective enforcement of existing rules.

Acknowledgments

We would like to thank the authors for their contributions, sharing their findings and insights into this crucial topic. The feedback and helpful comments of the invited reviewers were very valuable in improving the manuscripts and we would also like to thank them for their commitment and time. Finally, we would also like to thank all those at *Information Polity* who made this special issue possible. In particular, Kim Willems and Gabriela Ricci, who effectively managed the production process, and William Webster and Albert Meijer, the Editors-in-Chief, for their contributions and support in producing this special issue.

This special issue was edited by a group of researchers associated with the European Commission H2020 funded PANELFIT-project. PANELFIT stands for Participatory Approaches to a New Ethical and Legal Framework for ICT. The PANELFIT project has received funding under the European Union's H2020 research and innovation programme under grant agreement No 788039 (https://www.panelfit.eu/). The financial support from this project has also made it possible to publish the articles in this special issue as open access.